

21世纪高职高专规划教材
网络专业系列

计算机网络安全与管理

（第2版）

田庚林 田华 张少芳 编著

清华大学出版社

21世纪高职高专规划教材·网络专业系列

计算机网络安全与管理
（第2版）

田庚林　田　华　张少芳　编著

清华大学出版社
北　京

内 容 简 介

本书是面向高职高专计算机网络技术专业学生的教材。

本书以一个模拟网络工程为主线，分析网络工程中的安全管理需求，根据需求制定工程任务，按照任务介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。

本书共分7章，内容包括模拟网络工程环境和模拟网络工程中的项目介绍及网络安全基础、访问控制列表技术、网络地址转换、VPN技术、防火墙、局域网安全、网络管理技术。

本书可以作为高职高专计算机网络技术及相关专业学生的教材，也可以作为网络工程技术人员和本科院校学生的参考书。

图书在版编目(CIP)数据

计算机网络安全与管理/田庚林，田华，张少芳编著. --2版. --北京：清华大学出版社，2013
21世纪高职高专规划教材. 网络专业系列
ISBN 978-7-302-32407-2

Ⅰ. ①计… Ⅱ. ①田…②田…③张… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第096000号

责任编辑：刘 青
封面设计：傅瑞学
责任校对：刘 静
责任印制：

出版发行：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦A座 **邮 编**：100084
社 总 机：010-62770175 **邮 购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795764
印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：185mm×260mm **印 张**：20.25 **字 数**：461千字
版 次：2010年3月第1版 2013年10月第2版 **印 次**：2013年10月第1次印刷
印 数：1～ 000
定 价： .00元

产品编号：049875-01

出版说明

高职高专教育是我国高等教育的重要组成部分，担负着为国家培养并输送生产、建设、管理、服务第一线高素质技术应用型人才的重任。

进入21世纪后，高职高专教育的改革和发展呈现出前所未有的发展势头，学生规模已占我国高等教育的半壁江山，成为我国高等教育的一支重要的生力军；办学理念上，"以就业为导向"成为高等职业教育改革与发展的主旋律。近两年来，教育部召开了三次产学研交流会，并启动四个专业的"国家技能型紧缺人才培养项目"，同时成立了35所示范性软件职业技术学院，进行两年制教学改革试点。这些举措都表明国家正在推动高职高专教育进行深层次的重大改革，向培养生产、建设、管理、服务第一线真正需要的应用型人才的方向发展。

为了顺应当前我国高职高专教育的发展形势，配合高职高专院校的教学改革和教材建设，进一步提高我国高职高专教育教材质量，在教育部的指导下，清华大学出版社组织出版了"21世纪高职高专规划教材"。

为推动规划教材的建设，清华大学出版社组织并成立了"高职高专教育教材编审委员会"，旨在对清华版的全国性高职高专教材及教材选题进行评审，并向清华大学出版社推荐各院校办学特色鲜明、内容质量优秀的教材选题。教材选题由个人或各院校推荐，经编审委员会认真评审，最后由清华大学出版社出版。编审委员会的成员皆来自教改成效大、办学特色鲜明、师资实力强的高职高专院校、普通高校以及著名企业，教材的编写者和审订者都是从事高职高专教育第一线的骨干教师或专家。

编审委员会根据教育部最新文件和政策，规划教材体系，比如部分专业的两年制教材；"以就业为导向"，以"专业技能体系"为主，突出人才培养的实践性、应用性的原则，重新组织系列课程的教材结构，整合课程体系；按照教育部制定的"高职高专教育基础课程教学基本要求"，教材的基础理论以"必要、够用"为度，突出基础理论的应用和实践技能的培养。

本套规划教材的编写原则如下：

(1) 根据岗位群设置教材系列，并成立系列教材编审委员会；

(2) 由编审委员会规划教材、评审教材；

(3) 重点课程进行立体化建设，突出案例式教学体系，加强实训教材的出版，完善教学服务体系；

(4) 教材编写者由具有丰富的教学经验和多年实践经历的教师共同组成，建立"双师型"编者体系。

本套规划教材涵盖了公共基础课、计算机、电子信息、机械、经济管理以及服务等大类的主要课程,包括专业基础课和专业主干课。目前已经规划的教材系列名称如下:

• 公共基础课

公共基础课系列

• 计算机类

计算机基础教育系列
计算机专业基础系列
计算机应用系列
网络专业系列
软件专业系列
电子商务专业系列

• 电子信息类

电子信息基础系列
微电子技术系列
通信技术系列
电气、自动化、应用电子技术系列

• 机械类

机械基础系列
机械设计与制造专业系列
数控技术系列
模具设计与制造系列

• 经济管理类

经济管理基础系列
市场营销系列
财务会计系列
企业管理系列
物流管理系列
财政金融系列
国际商务系列

• 服务类

艺术设计系列

本套规划教材的系列名称根据学科基础和岗位群方向设置,为各高职高专院校提供"自助餐"形式的教材。各院校在选择课程需要的教材时,专业课程可以根据岗位群选择系列;专业基础课程可以根据学科方向选择各类的基础课系列。例如,数控技术方向的专业课程可以在"数控技术系列"选择;数控技术专业需要的基础课程,属于计算机类课程的可以在"计算机基础教育系列"和"计算机应用系列"选择,属于机械类课程的可以在"机械基础系列"选择,属于电子信息类课程的可以在"电子信息基础系列"选择。依此类推。

为方便教师授课和学生学习,清华大学出版社正在建设本套教材的教学服务体系。本套教材先期选择重点课程和专业主干课程,进行立体化教材建设:加强多媒体教学课件或电子教案、素材库、学习盘、学习指导书等形式的制作和出版,开发网络课程。学校在选用教材时,可通过邮件或电话与我们联系获取相关服务,并通过与各院校的密切交流,使其日臻完善。

高职高专教育正处于新一轮改革时期,从专业设置、课程体系建设到教材编写,依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议,并向我们推荐优秀选题。反馈意见请发送到E-mail:gzgz@tup.tsinghua.edu.cn。清华大学出版社将对已出版的教材不断地修订、完善,提高教材质量,完善教材服务体系,为我国的高职高专教育出版优秀的高质量的教材。

高职高专教育教材编审委员会

第 2 版前言

本书以一个模拟网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案的配置。本书内容以工程需求为主，同时还兼顾了知识体系的完整性与系统性。为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。第 2 章至第 7 章的每章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，增强学生的动手能力与实践技能。

本书在第 1 版的基础上进行了部分修改，除了根据教学中的反馈信息对内容排列顺序进行调整之外，主要增加了 H3C 设备的内容。第 1 版主要以 Cisco 设备为例，但目前国内企业所用的网络设备大都以国内厂商的设备为主，而在网络安全配置方面，不同厂家的设备配置方法差异较大，所以在第 2 版中，同时兼顾了 Cisco 设备及 H3C 设备。书中主要以 H3C 设备配置为例进行介绍，而后给出 Cisco 设备的配置方案。

本书共分 7 章。第 1 章介绍模拟网络工程环境和模拟网络工程中的项目介绍及网络安全基础；第 2 章介绍访问控制列表技术，根据工程任务安全需求分析，解决网络边界访问控制配置问题；第 3 章介绍网络地址转换，根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题；第 4 章介绍 VPN 技术，根据工程任务安全需求分析，解决利用 Internet 线路进行安全通信配置问题；第 5 章介绍防火墙，根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题；第 6 章介绍局域网安全，根据工程任务安全需求分析，解决局域网中安全配置问题；第 7 章介绍网络管理技术，包括基本网络管理知识和常用的网络管理工具。附录中介绍了如何利用网络模拟器 GNS3 搭建模拟实训环境、iMC 安装指导，并配有各章习题参考答案。

本书由田庚林主持编写，具体内容由田华、张少芳编写完成。其中田庚林主要参与了内容的组织策划和统稿审订工作，第 6 章、第 7 章由田华编写，其余部分由张少芳编写。

由于计算机网络技术发展更新较快，编者水平有限，书中的不足之处望广大读者批评指正。作者 E-mail：tiangl163@163.com。

编　者

2013 年 6 月

第1版前言

本书是一本面向高等职业教育的教材，是计算机网络技术专业系列教材之一。

在计算机网络技术专业建设中，从网络工程、网络管理岗位需求出发，我们将专业技能重点放在网络技术和网站技术两个方面。该专业系列教材中，将网络技术分为《计算机网络技术基础》、《计算机网络集成技术》、《计算机网络安全与管理》和《网络操作系统》4门课程；网站技术主要包括《网页制作工具》、《网络数据库》、《动态网站技术》和《.NET网站技术》4门课程。本书主要介绍网络安全技术和基本的网络管理知识与基本管理技能。

本书以一个模拟的网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。本书内容既以工程需求为主，同时还照顾了知识体系的完整性与系统性。为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出了一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。第2章至第7章的每章章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，提高学生的动手能力与实践技能。

本书共分7章。第1章介绍模拟网络工程环境和模拟网络工程中的网络安全与管理需求分析；第2章介绍访问控制列表技术，根据工程任务安全需求分析，解决网络边界访问控制配置问题；第3章介绍局域网安全，根据工程任务安全需求分析，解决局域网中安全配置问题；第4章介绍网络地址转换技术，根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题；第5章介绍VPN技术，根据工程任务安全需求分析，解决利用Internet线路进行安全通信配置问题；第6章介绍防火墙技术，根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题；第7章介绍网络管理技术，包括基本网络管理知识和常用的网络管理工具。附录中介绍了如何利用网络模拟器GNS3搭建模拟实训环境。本书中的网络设备都是以Cisco为例介绍的。

本书由田庚林主持编写，具体章节由田华、张少芳编写完成。其中，田庚林主要参与了内容的组织策划和统稿审订工作，第3章和第4章由张少芳编写完成，其余章节由田华编写完成。

由于计算机网络技术发展更新较快，编者水平有限，书中的不足之处望广大读者批评指正。编者E-mail：tiangl163@163.com。

编　者

2009年12月

目 录

第 1 章

项目介绍及网络安全基础

随着网络技术的不断发展和普及，网络安全技术也越来越受到人们的关注。人们都知道如果一台PC仅仅安装了操作系统，而没有安装任何杀毒软件、防火墙（单机软件）等安全防护软件，那么可能在很短的时间内系统就会因为受到病毒等的攻击而瘫痪，而网络作为一个开放的信息系统同样会存在诸多的安全隐患。在实际中，任何一个计算机网络系统，特别是较大型的企业网络系统，为保证其安全、可靠地运行，必须建立相应的网络安全与管理方案，以减少各种潜在网络安全风险和网络性能瓶颈对信息系统正常运行的影响。本书以一个典型的跨地区公司网络系统为例，按照实际网络工程项目过程，先分析其中的网络安全与管理问题，然后介绍解决这些问题所需的知识和技术，最后给出这些问题的相应的解决方案。

1.1 网络安全与管理项目介绍

1.1.1 模拟公司网络环境

1. 企业网络应用情况

某大型新兴产业公司为提高生产效率，拟新建联通各地分公司的计算机网络。该公司的总公司及其直属3个分支机构在A市，并在B市和C市分别设有一个分公司和两个分支机构。总公司和分公司主要负责产品的研发和生产，设有管理部门、研发部门、市场部门、售后服务部门和生产部门。各分支机构主要负责产品销售和售前、售后服务，设有市场部门、售后服务部门和管理部门。

公司所建网络将主要承载公司内部OA、邮件、FTP、远程教育等系统和面向公众提供服务的电子商务网站系统。受业务发展、系统性能等诸多方面因素影响，以上网络应用系统设计在总公司、分公司分别设有网络应用及数据库服务器，而在分支机构只设网络终端。

2. 企业网络拓扑结构

全公司的网络拓扑结构如图1-1所示。总公司与分公司利用电信专线互联，而为节约线路成本，总/分公司与其下属分支机构通过宽带线路接入本地Internet实现互联。

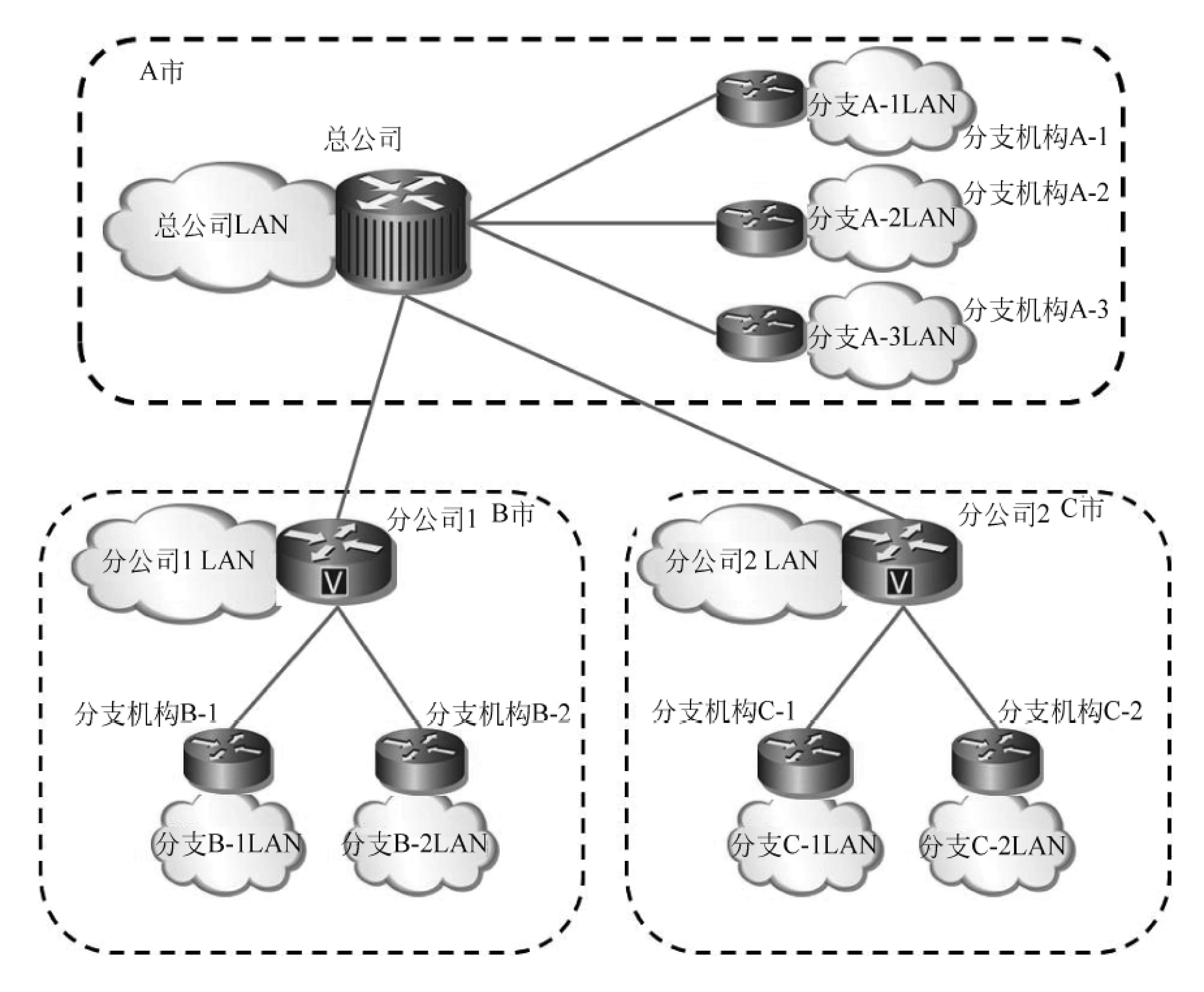


图 1-1 模拟公司网络拓扑结构示意图

总公司局域网的网络拓扑结构按照网络应用需求分为核心、汇聚、接入3层,图1-2为总公司局域网网络拓扑结构示意图。为了保证系统安全可靠性,在各交换机上使用了双冗余线路设计。

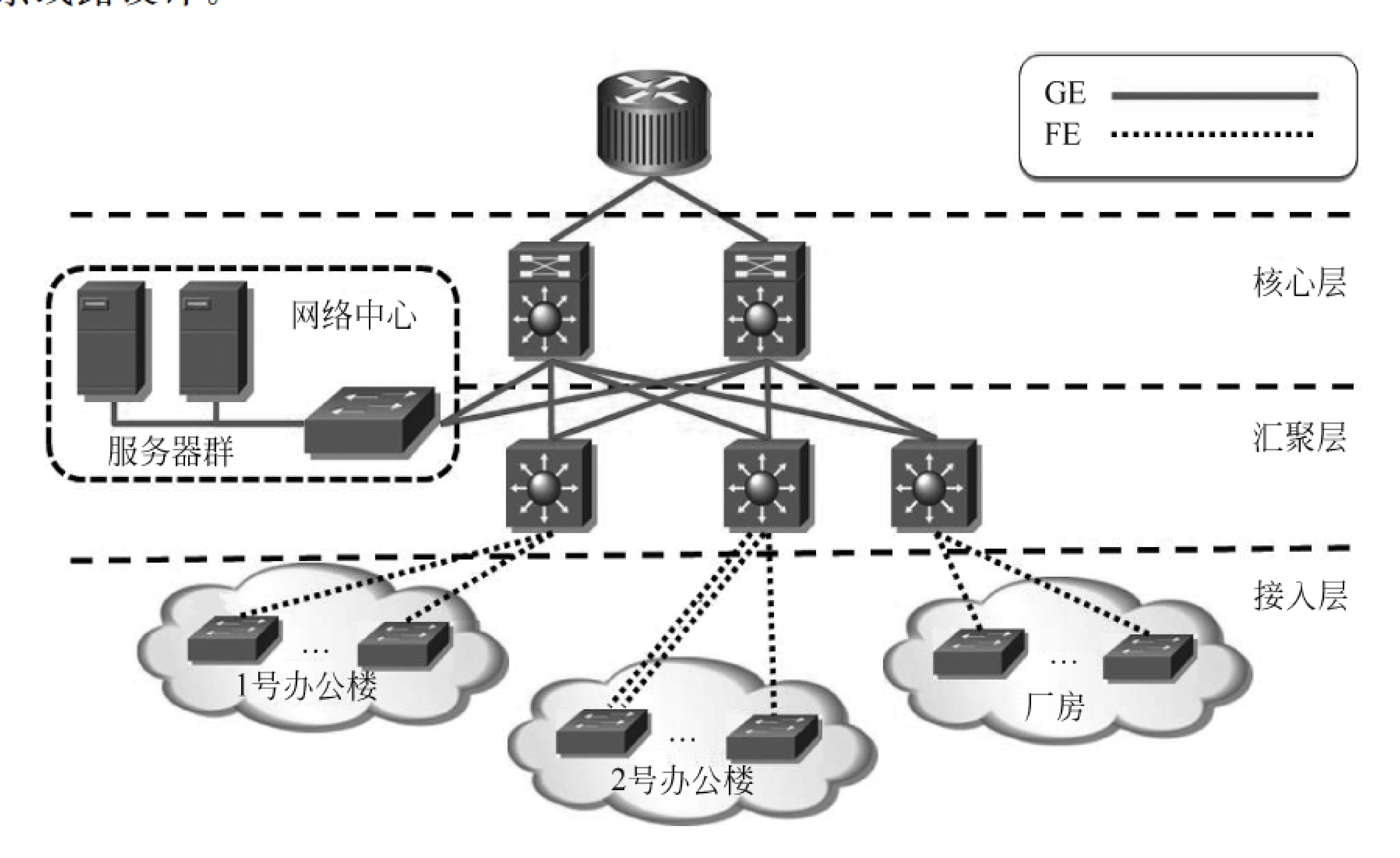


图 1-2 总公司局域网网络拓扑结构图

分公司在局域网结构、链路冗余等方面与总公司类似。但分支机构 B-1、C-1 网络规模较大，而分支机构 B-2、C-2 网络规模较小，分支机构的网络拓扑结构分别如图 1-3 所示。

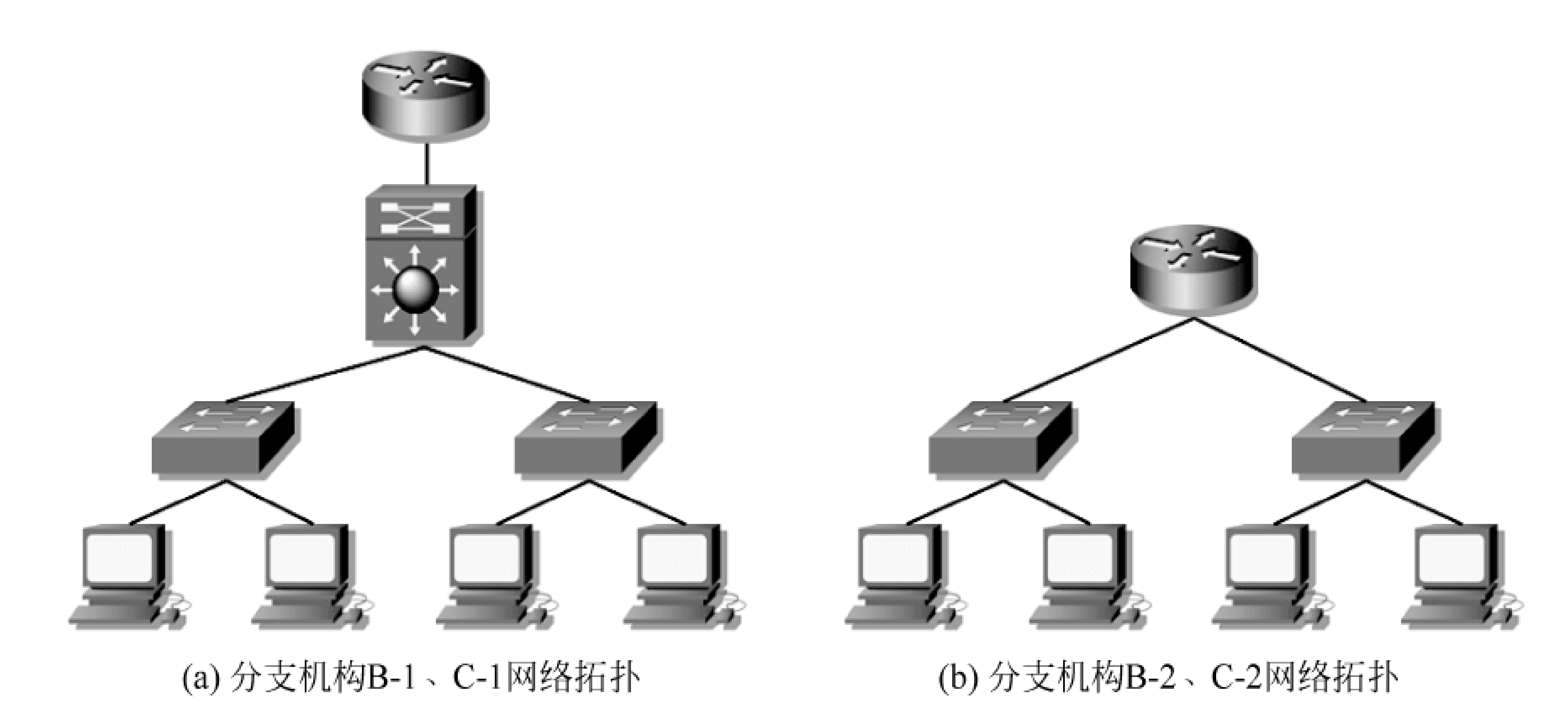


图 1-3　分支机构网络拓扑结构图

1.1.2　模拟公司网络安全及管理需求

1. 网络安全需求

目前计算机网络面临着多方面的安全威胁，例如物理安全威胁、网络通信威胁、网络服务威胁、网络管理威胁等，模拟公司网络也不能例外。从模拟公司网络环境和业务需求分析可以发现，要保证该网络安全运行，需要解决以下网络安全问题。

(1) 由于连接到 Internet，所以必须解决来自 Internet 的网络入侵和攻击问题。

(2) 模拟公司与分支机构间使用 Internet 线路通信，必须解决通信数据安全问题。

(3) 由于公司租用的 IP 地址有限，随着企业网络规模发展，必须解决公司网络中 IP 地址资源不足的问题。

(4) 模拟公司网络不是单纯的生产网络，办公局域网的接入使得网络管理人员必须面对局域网中各种潜在安全威胁，如病毒问题、非授权访问网络资源问题、非授权变更网络结构等。

2. 网络管理需求

要保证模拟公司网络安全、可靠地运行，必须对网络进行管理和维护。在网络管理过程中，需要解决以下问题。

(1) 根据网络需求变化，使用工具对网络进行配置、调整。

(2) 当网络发生故障时，能够发现、跟踪故障现象，记录故障状态信息，分析故障原因，解决网络故障。

(3) 监控、记录网络性能变化，根据需求适当调整网络，以提高网络性能。

(4) 监控、记录网络受到安全威胁的情况，检查网络可能存在的安全漏洞或隐患，并通过访问控制等手段对网络的薄弱环节进行改善。

1.1.3 网络安全与管理实验环境

本书将根据以上网络安全及管理方案基本设计思路,逐个解决模拟公司网络中的安全及管理方面的问题,介绍相关知识,提出解决方案,完成相应系统配置。另外,在每一章后面都给出了相关知识的实验,下面对实验环境进行简单的介绍。

1. 物理实验环境

物理实验环境中共有8个学习岛,每一个学习岛由1台机柜和5台计算机组成。实验环境的物理规划如图1-4所示。

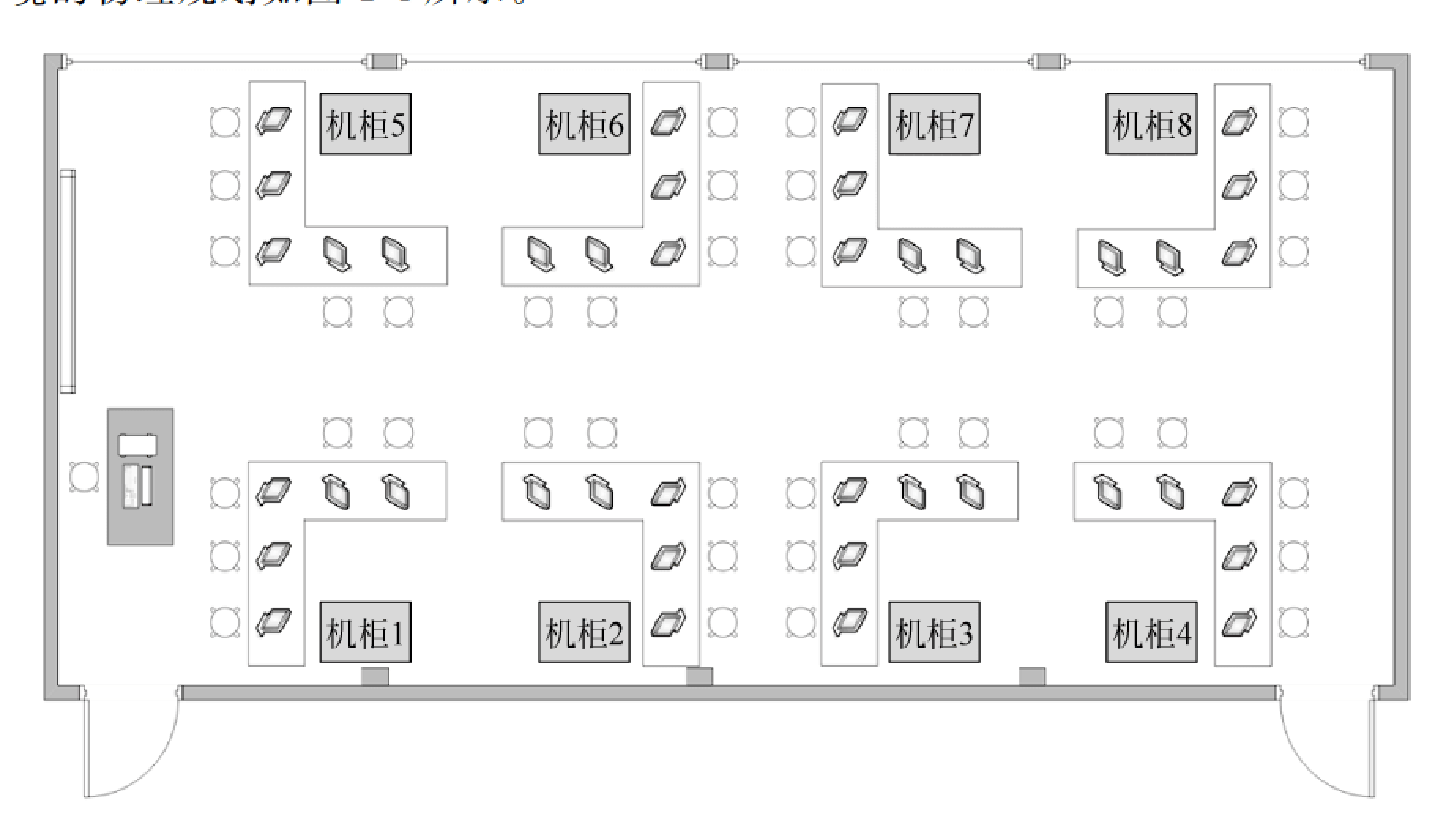


图1-4 实验环境物理规划图

为满足实验的需要,每台机柜中包含的设备如下:

(1) 路由器4台;

(2) 二层交换机2台;

(3) 三层交换机2台;

(4) 防火墙1台。

由于在本书中涉及H3C和Cisco两种设备的配置,因此读者可以根据具体情况配备H3C设备或Cisco设备,Cisco设备也可以通过Packet Tracer或GNS3等模拟器软件来代替。在本书中H3C设备和Cisco设备配置使用相同的网络实验环境,但两个厂商对接口的命名方式存在区别,在书中所有的网络拓扑图中给出的接口均以H3C设备的命名方式进行命名,Cisco设备接口与H3C设备接口的对应表如表1-1所示。

表1-1 Cisco与H3C接口名称对应表

Cisco设备接口	H3C设备接口
FastEthernet0/0	Ethernet0/0
FastEthernet0/1	Ethernet0/1
Serial0/0	Serial1/0
Serial0/1	Serial2/0

2. 逻辑实验环境

(1) 逻辑网络拓扑与 IP 地址规划

为使各个学习岛可以访问外部网络,在实验网络的出口处使用一台路由器和一台三层交换机来进行校园网与实验网络以及实验网络内各个学习岛网络之间的连接。实验网络具体的逻辑拓扑与 IP 地址规划如图 1-5 所示。

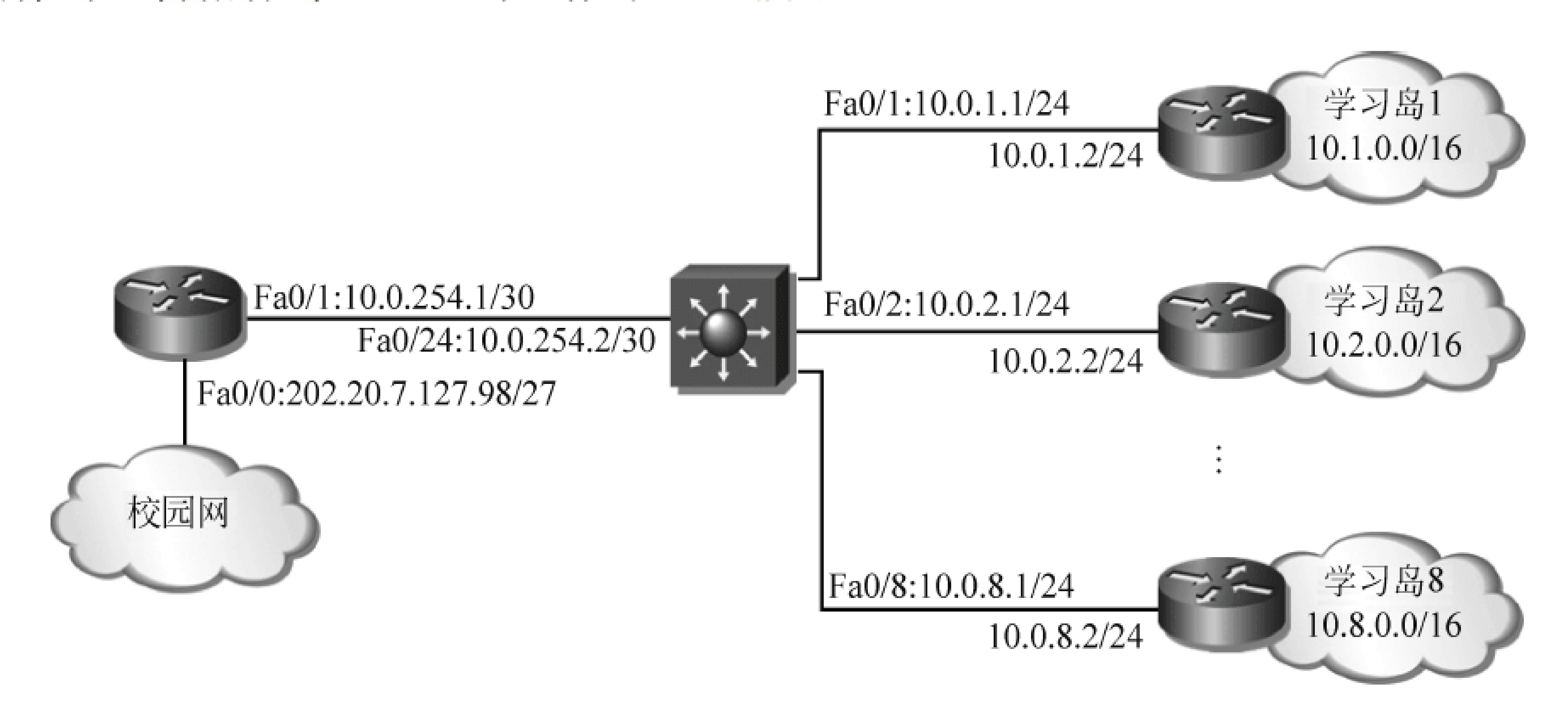


图 1-5　实验网络的逻辑拓扑与 IP 地址规划图

从图 1-5 可以看出,学习岛 1～学习岛 8 的 WAN 接口分别连接到了出口三层交换机的 Fa0/1～Fa0/8 接口上,出口三层交换机向上连接到出口路由器上,出口路由器向上连接到校园网。

在 IP 地址的规划上,具体的规划原则和 IP 地址分配情况如下:

① 三层交换机与各个学习岛之间链路分配的 IP 网段为 10.0.x.0/24,其中 x 为学习岛的编号。当学习岛上的实验网络拓扑为计算机通过二层网络设备连接到 WAN 接口上时,为计算机分配 10.0.x.0/24 网段的 IP 地址,网关为 10.0.x.1。

② 为每一个学习岛预留的 IP 网段为 10.x.0.0/16。当学习岛上的实验网络拓扑为通过三层网络设备连接到 WAN 接口上时,实验网络内可以使用网段 10.x.0.0/16,并可以根据实验的需求将 10.x.0.0/16 划分成若干个子网。

为实现 10.x.0.0/16 到达其他网段的网络联通性,在出口三层交换机上为每一个学习岛的预留网段均配置了一条静态路由,为学习岛 1 配置的静态路由如下:

```
Switch(config)#ip route 10.1.0.0 255.255.0.0 10.0.1.2
```

从上面的配置命令可以看出,指定的下一跳地址为 10.0.x.2,因此学习岛上与 WAN 接口(即与出口三层交换机)相连的三层网络设备接口 IP 地址一定要配置为 10.0.x.2。另外需要注意的是,在出口三层交换机上只能使用静态路由来实现各个学习岛的联通性,而不能使用动态路由。如果使用了动态路由协议,例如 RIPv2,则在学习岛上的实验环境中也存在 RIPv2 的情况下,任何一个学习岛都会学习到其他学习岛内部的实验环境路由,从而会造成学生实验的混乱。

在出口三层交换机上,除了为每一个学习岛配置了一条静态路由外,还配置了一条指

向出口路由器的默认路由。在出口路由器上共配置了两条路由,一条为指向出口三层交换机目的网络为10.0.0.0/8的静态路由;另一条为指向校园网的默认路由。

(2) 实验网络的安全策略

① 地址转换策略。通过配置静态和默认路由,实现了各个学习岛之间的联通性,但是由于使用私有地址段10.0.0.0/8的关系,各个学习岛依然无法访问外部网络。如果要实现对外部网络的访问,就必须在出口路由器上配置网络地址转换。由于校园网只给网络实验室分配了一个合法IP地址202.207.127.98,并且该地址已经被分配给了出口路由器连接校园网的接口Fa0/0,因此需要配置基于接口的地址转换,即Easy IP。具体的配置命令如下:

```
Router(config)#ip access-list standard sacl-pat
Router(config-std-nacl)#permit 10.0.0.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list sacl-pat interface FastEthernet0/0 overload
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat outside
```

配置完成后,各个学习岛即可通过唯一的内部全局地址202.207.127.98访问外部网络。

② 访问控制策略。对于访问外部网络的需求,一方面学生需要访问校园网内和Internet上的一些服务器,例如访问教务处的网站进行选课和成绩查询、访问人事考试中心的网络进行网络管理员认证的报名和成绩查询、访问百度进行实验联通性验证等;另一方面又需要防止学生在实验室进行上网聊天、打游戏或看电影等与学习无关的事情。这就需要在出口路由器上进行访问控制列表的配置来实现对网络的访问控制。具体的配置命令如下:

```
Router(config)#ip access-list extended in2out
Router(config-ext-nacl)#permit ip any 202.207.120.0 0.0.7.255
//允许访问校园网
Router(config-ext-nacl)#permit ip any host 202.99.160.68
//允许访问联通的DNS服务器
Router(config-ext-nacl)#permit ip any host 121.28.90.107
Router(config-ext-nacl)#permit ip any host 219.148.28.212
//允许访问河北省人事考试中心网站
Router(config-ext-nacl)#permit ip any host 61.135.169.105
Router(config-ext-nacl)#permit ip any host 61.135.169.125
//允许访问百度首页
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip access-group in2out in
```

上面给出的访问控制列表仅供参考,可以根据具体的访问需要随时进行调整。

1.2　网络安全的概念

网络安全从本质上讲就是网络上的信息安全，是指网络系统的硬件、软件以及系统中的数据受到保护，不受偶然的或者恶意的因素而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面互相补充、缺一不可。技术方面主要侧重于如何防范外部非法攻击；管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

1.3　常见网络攻击方式

1.3.1　勘测攻击

勘测攻击是一种对网络进行扫描或窃听，从而获得网络拓扑、网络中主机或网络设备运行应用软件情况的攻击方式，往往是恶意用户对网络实施攻击的前奏。勘测攻击的两种常见类型是扫描攻击和窃听攻击。

1. 扫描攻击

常见的扫描攻击可以分为 IP 地址扫描和端口扫描。

IP 地址扫描是指通过 ping 网络的直接广播地址或者 ping 网络中的每个 IP 地址，以及使用 IP 地址扫描工具(例如，IPScanner、深度活跃 IP 扫描器等)对特定网段进行 IP 地址扫描，从而发现网络中存活的 IP 地址。

端口扫描是指使用端口扫描工具(例如，Superscan、Fluxay 等)通过测试是否可以与网络中的主机建立各类服务连接，来探测目标主机的哪些端口处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。

2. 窃听攻击

窃听攻击是指恶意用户通过各类嗅探、监听软件(例如，Wireshark、QQ Sniffer 等)从网络中获取用户的通信信息，从而获知用户的账号、密码以及其他机密信息等。由于窃听攻击一般需要在本地网络中实施，因此恶意用户往往会先攻陷内部网络的一台主机，然后在这台主机上运行嗅探、监听软件，从而达到窃听攻击的目的。

1.3.2　访问攻击

常见的访问攻击类型包括未授权访问攻击、数据操纵攻击以及会话攻击等。

1. 未授权访问攻击

未授权访问攻击是指通过口令暴力破解、社会工程学窃取口令等试图获得访问网络

权利的攻击方式。

2. 数据操纵攻击

数据操纵攻击是指对网络服务提供的数据内容进行修改从而达到攻击目的，例如，改变网页内容，在其中嵌入非法插件、Java 小程序等。

3. 会话攻击

会话攻击是指在网络的会话层实施的攻击，包括会话欺骗攻击、会话重放攻击和会话劫持攻击等。

会话欺骗攻击是指通信会话中假冒其他 IP 地址的攻击行为。据统计，大约 65% 的会话欺骗攻击会使用 bogon 地址(即未被分配的地址)，包括保留地址、私有地址等；另外恶意用户常常假冒内网合法主机发动会话欺骗攻击。

会话重放攻击是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器，如图 1-6 所示。为了抵御会话重放攻击，现在的身份认证一般采用"挑战应答"(Challenge/Response)方式，例如 PPP 中的 CHAP 认证、IEEE 802.1x 认证等。

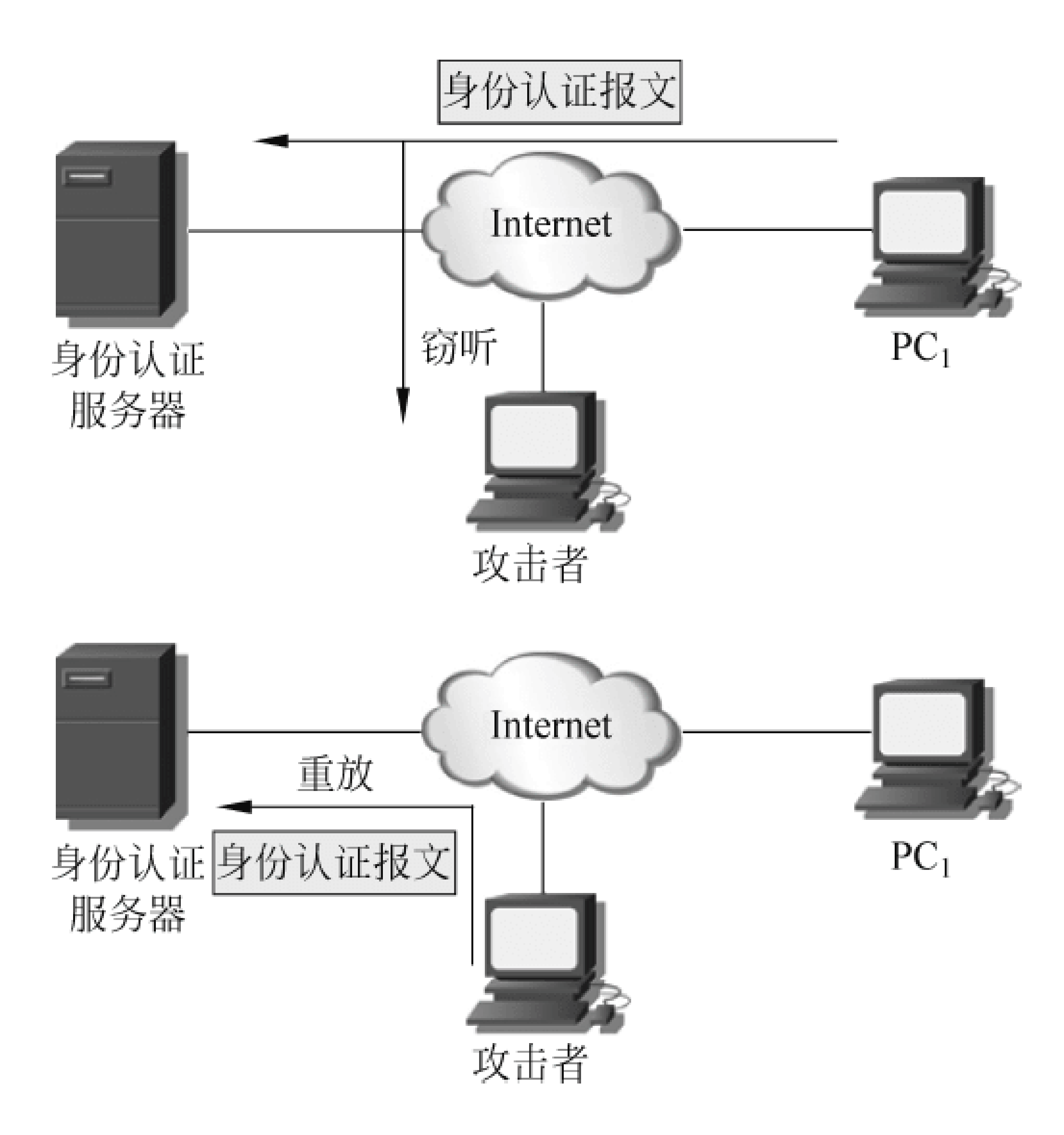


图 1-6 会话重放攻击

会话劫持攻击是指在一次正常的会话过程当中，攻击者作为第三方参与到其中，它可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。会话劫持攻击按照攻击类型可以分为中间人攻击(如图 1-7 所示)和注射式攻击两种，而按照攻击方式可以分为主动劫持和被动劫持两种。在被动劫持中攻击者是在后台监视双方会话的数据流并从中获得敏感数据；而主动劫持则是将会话当中的某一台主机踢下线，然后由攻击者取代并接管会话。

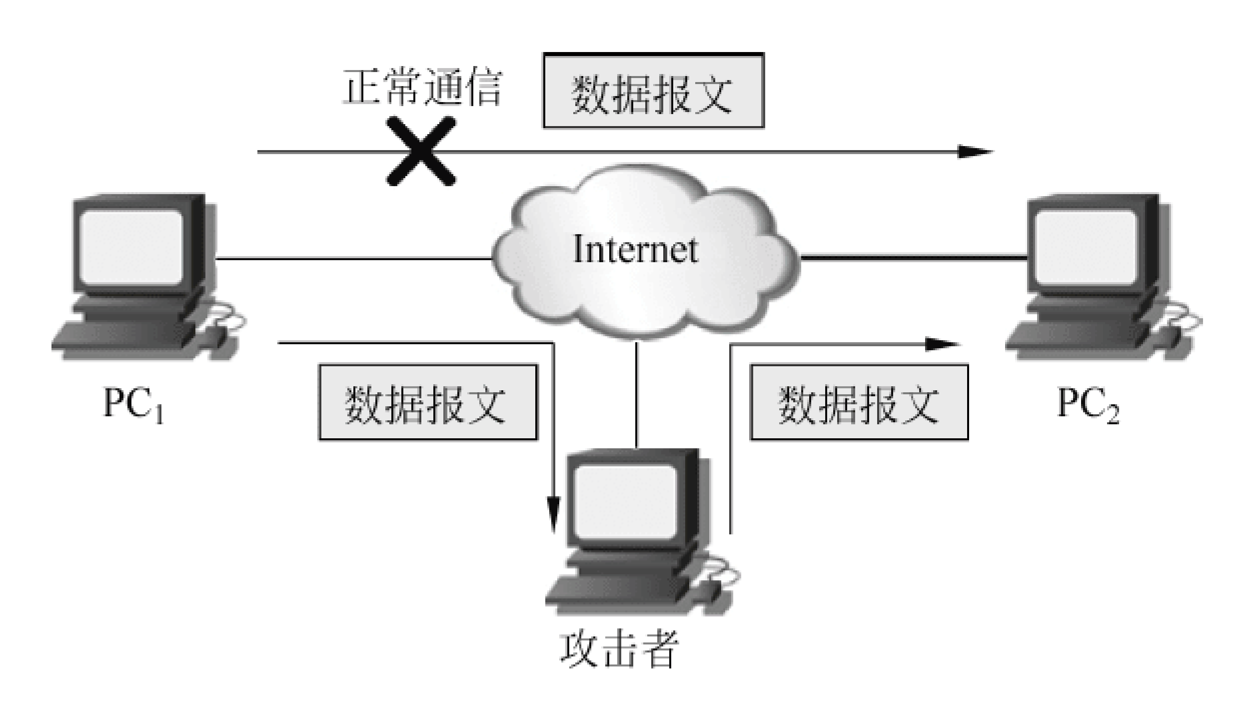


图 1-7　会话劫持攻击

1.3.3　拒绝服务攻击

拒绝服务攻击(Denial of Service,DoS)是通过向网络中的网络设备、计算机等发送大量消耗、占用其资源的流量,使被攻击网络或主机无法及时接收并处理外界请求,从而导致无法提供正常网络服务的攻击方式。DoS 攻击的具体表现方式有以下 3 种:制造大量的无用数据来占用网络带宽,造成通往被攻击主机的网络拥塞,从而使被攻击主机无法正常和外界通信;利用被攻击主机提供的服务或传输协议上处理重复连接的缺陷,高频率地发出攻击性的重复服务请求,使被攻击主机无法及时处理其他正常的请求,例如 SYN 洪水(SYN Flood)攻击;利用被攻击主机所提供服务程序或传输协议的本身实现缺陷,反复发送畸形的攻击数据引发系统错误地分配大量系统资源,使主机处于挂起状态甚至死机,例如死亡之 ping(Ping of Death)攻击和泪滴(Tear Drop)攻击等。下面对典型的几种 DoS 攻击进行简要介绍。

1. SYN 洪水攻击

SYN 洪水(SYN Flood)攻击是一种利用 TCP 协议的安全漏洞进行的 DoS 攻击。我们知道 TCP 协议在建立连接时有一个 3 次握手的过程。第一次握手是客户端发送 SYN 请求数据报文给服务器端;第二次握手是服务器端在接收到客户端的 SYN 请求后将分配一定的资源用来准备建立连接,并同时返回一个 SYN-ACK 数据报文;第 3 次握手是客户端接收到服务器端返回的 SYN-ACK 数据报文后,向服务器端发送一个 ACK 报文,建立 TCP 连接。SYN 洪水攻击正是利用了 TCP 3 次握手过程中存在的漏洞,一般攻击者会使用伪造的源 IP 地址向被攻击服务器发送大量的 SYN 请求报文,被攻击服务器在进行第二次握手响应后会等待客户端的 ACK 报文来建立 TCP 连接。但是由于源 IP 地址欺骗的原因被攻击服务器实际上不会接收到任何的 ACK 响应报文,从而使被攻击服务器的大量资源被这种 TCP 半开连接占用,导致被攻击服务器无法对正常的 TCP 连接请求进行响应。

SYN 洪水攻击是一种典型以小搏大的攻击,即使用自己的少量资源来占用对方大量的资源。并且由于伪造源 IP 地址的原因,使 SYN 洪水攻击很难找到攻击者。

2. 死亡之 ping 攻击

死亡之 ping(Ping of Death)攻击是利用 ICMP 协议的漏洞进行的 DoS 攻击。ICMP

协议其中一个重要的功能就是通过“请求/应答”报文对来测试目标主机是否存活或者与目标主机之间的联通性。在TCP/IP协议簇的RFC文档中对ICMP数据报文的大小有着严格规定,一般操作系统的TCP/IP协议栈对于ICMP数据报文的大小都规定为64KB,并且在对ICMP数据报文的标题头进行读取之后,根据该标题头里包含的信息来为有效载荷生成缓冲区。死亡之ping攻击通过产生畸形的ICMP echo-request数据报文,声称自己的尺寸超过ICMP上限,也就是加载的尺寸超过64KB上限,从而使未采取保护措施的系统出现内存分配错误,导致TCP/IP协议栈崩溃,并最终导致接收方死机。

作为一种比较老的攻击方式,目前所有标准的TCP/IP实现均可以处理超大尺寸的ICMP echo-request数据报文,并且大多数的防火墙都可以自动过滤死亡之ping攻击。

3. Smurf 攻击

Smurf攻击是一种基于ICMP echo-reply数据报文的洪水攻击,属于反射拒绝服务攻击。在Smurf攻击中,攻击者会伪造ICMP的echo-request数据报文,其中报文的源IP地址为被攻击主机的IP地址,而目的IP地址为某一个网络的直接广播地址或者本网段的受限广播地址。在攻击者发送出伪造的ICMP echo-request数据报文后,目的网段中的所有主机都会收到该报文,并向被攻击主机发送ICMP echo-reply数据报文,从而导致被攻击主机瞬间被大量的ICMP echo-reply数据报文淹没。Smurf攻击属于典型的“借刀杀人”攻击方式,而ICMP echo-request数据报文中目的网络的所有主机均充当了攻击者的角色,因此Smurf也是一种典型的DDoS攻击。

对于Smurf攻击的防范,首先应该禁用网关设备的IP广播功能,从而避免伪造的ICMP echo-request数据报文向目的网络传播。当然,如果ICMP echo-request数据报文的目的IP地址为本网段的受限广播地址,即在本网段内发动的Smurf攻击,则禁用网关设备的IP广播功能不会起到防范作用,此时只能在操作系统上进行相应设置,防止计算机对IP广播请求作出响应。

1.3.4 分布式拒绝服务攻击

与拒绝服务攻击一对一的攻击方式不同,分布式拒绝服务攻击(Distributed Denial of Service,DDoS)是一种分布、协作的大规模攻击方式。DDoS攻击借助于客户/服务器技术,将多台受控制的傀儡主机联合起来作为攻击平台,对一个或多个目标发动DoS攻击,从而成倍地提高拒绝服务攻击的威力。

在DDoS攻击的体系结构中共有4种不同的角色,如图1-8所示。

1. 攻击者

攻击者是整个DDoS攻击中的主控台,它负责向主控端发送攻击命令。与DoS中的攻击者不同的是,DDoS的攻击者对计算机的配置和网络带宽的要求并不高,只要能够向主控端发送攻击命令即可。

2. 主控端

主控端即控制傀儡机,主控端是攻击者非法侵入并控制的一些主机。攻击者会在主控端上安装DDoS的主控程序,通过主控程序主控端可以接收来自攻击者的攻击命令,并将这些攻击命令发送到代理端,从而控制代理端的攻击。

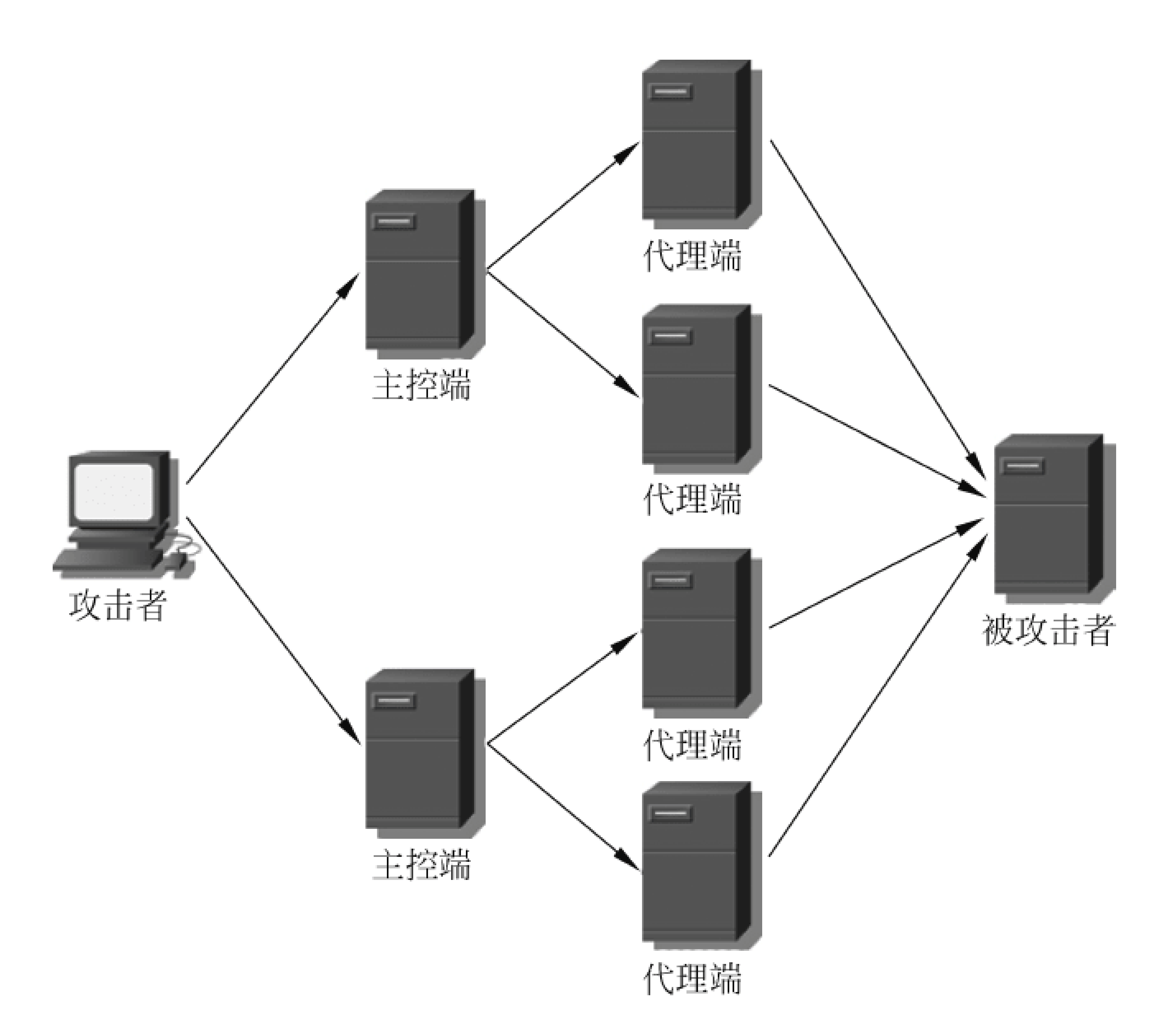


图 1-8　DDoS 攻击的原理

3. 代理端

代理端即攻击傀儡机,代理端同样也是攻击者非法侵入并控制的一些主机。攻击者会在代理端安装并运行 DDoS 的攻击程序,它可以接收并运行主控端发来的攻击命令,对被攻击者实施攻击。代理端是攻击的具体执行者。

4. 被攻击者

被攻击者即 DDoS 攻击的受害者,一般多为对外提供访问服务的网站、邮件服务器以及数据库系统等。

在 DDoS 攻击的过程中,攻击者首先会在 Internet 上寻找存在漏洞的主机,入侵其系统并在其上安装主控程序或攻击程序,使其成为主控端或代理端;然后由攻击者控制主控端向代理端发送攻击命令进行 DDoS 攻击。由于直接对被攻击者进行攻击的代理端是由主控端而不是攻击者直接控制,因此 DDoS 攻击的攻击者一般很难被发现。典型的 DDoS 攻击有 TFN(Tribe Flood Network)、TFN2K(Tribe Flood Network 2000)、Trinoo 等。

1.4　小结

本章主要对书中使用到的网络安全与管理的项目进行了介绍,对项目中的网络安全与网络管理的需求进行分析,并给出网络安全与管理的具体实验环境。另外,本章还对网络安全的概念以及常见的网络攻击方式进行了介绍,并简要介绍了网络安全关注的内容,为后续章节进行具体安全技术的介绍进行铺垫。

1.5 习题

1. 什么是网络安全？为什么说网络安全是一门综合性的学科？
2. 扫描攻击有哪两种形式？其目的分别是什么？
3. 什么是会话劫持攻击？按照攻击方式的不同可以将其分为哪两种？
4. 什么是拒绝服务攻击？典型的拒绝服务攻击有哪些？
5. 在分布式拒绝服务攻击的体系结构中有几种不同的角色？其作用分别是什么？

第 2 章

访问控制列表技术

本章任务： 根据工程任务安全需求分析，解决网络边界访问控制配置问题。

必备知识： (1) 无状态访问控制列表技术。

(2) 有状态访问控制列表技术。

学习目标： 利用访问控制列表技术完成模拟公司分支机构网络边界访问控制配置，防御外网攻击。

2.1 模拟公司分支机构网络边界安全任务分析

如图 2-1 所示，模拟公司各分支机构网络通过 Internet 与模拟公司其他网络相连，各分支机构网络内设有可 24h 连接到 Internet 的邮件服务器，周一至周五使用端口 3000～3010 通过 Internet 连接总/分公司的应用服务器，24h 可通过 Internet SSH 连接远程管理的网络设备。

由于 Internet 网络的开放性，各分支机构网络面临着恶意用户勘测攻击、访问攻击、DoS 攻击以及 DDoS 攻击的危险。为保护分支机构网络的安全，需要在分支机构的边界路由器上进行访问控制列表的配置。具体的安全配置方案如下：

(1) 在网络边界上配置有状态的访问控制列表过滤来自 Internet 到内网主机或服务器的所有 ICMP echo 报文，来防御利用 ping 进行的扫描攻击。

(2) 在网络边界上配置基本访问控制列表，过滤所有来自 Internet 的源地址为 bogon 地址或内网地址的访问，防御 IP 欺骗攻击。

(3) 在网络边界上配置基于有状态的访问控制列表，防范 DoS 攻击。包括限制来自 Internet 的 ICMP 报文进入内部网络，以防范 Smurf；限制 Internet 对分支机构网络主机的主动 TCP 连接、UDP 连接，以防范 TCP SYN 等。

(4) 在网络边界上配置高级访问控制列表，防范使用特定协议消息、特定端口的 DDoS 攻击。包括阻塞 ICMP echo-reply 消息，以抵御 TFN 攻击；禁止 TCP、UDP 1524、27444、27665、16660、65000、31335 端口的流量，以防御 Trinoo 等 DDoS 攻击；禁止 TCP 端口 6665～6669 的 IRC 流量以防御 Trinity 攻击；禁止常见特洛伊木马使用的特定端口。

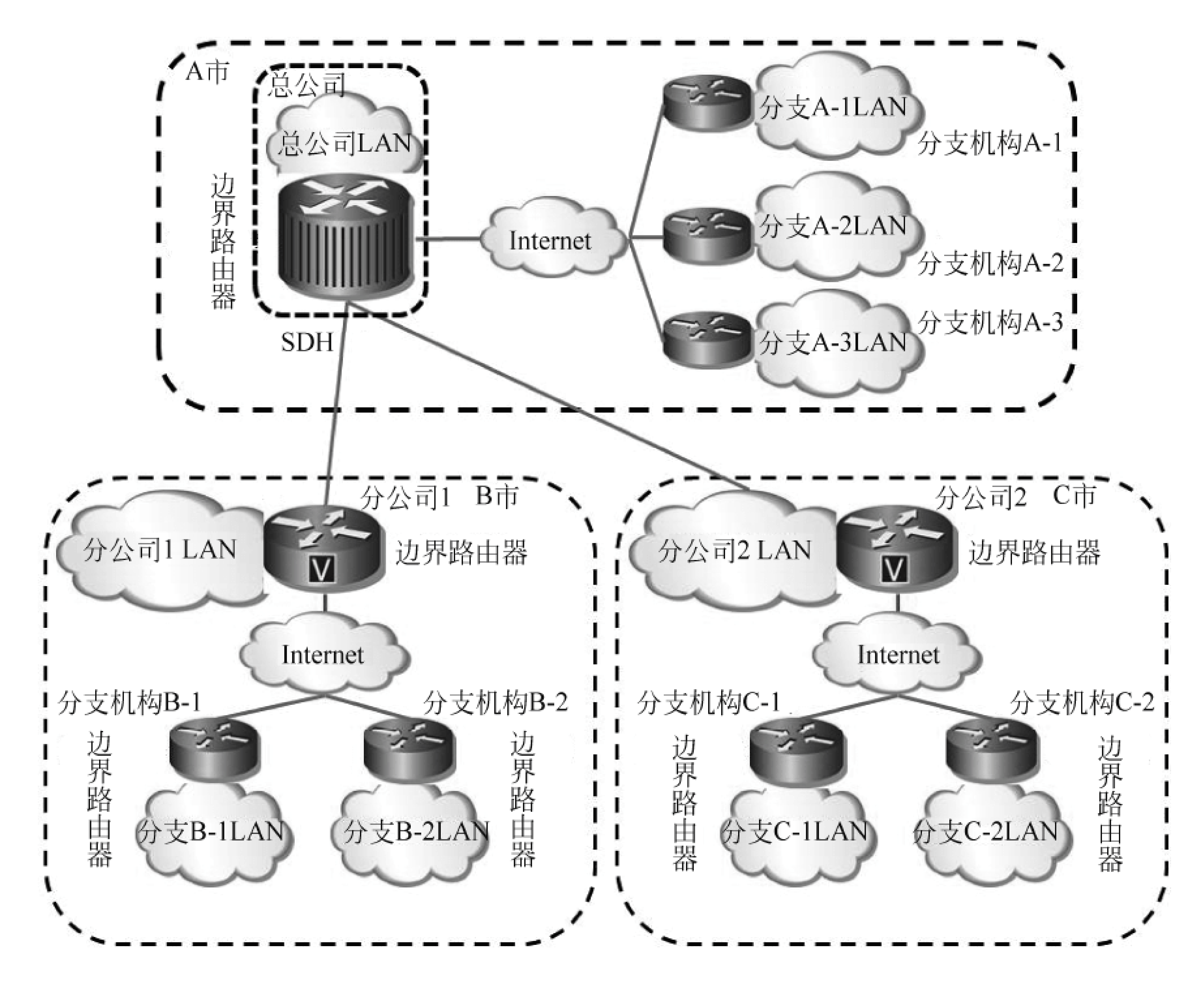


图 2-1 模拟公司网络间连接拓扑示意图

方案中提及的 bogon 地址,可以检索 http://www.cymru.com/Documents/bogon-dd.html 获得;常见木马端口可从 http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html 获得。表 2-1 显示了 Internet 上的 bogon 地址。

表 2-1 bogon 地址示例

网络地址	子网掩码	网络地址	子网掩码
0.0.0.0	254.0.0.0	100.0.0.0	252.0.0.0
2.0.0.0	255.0.0.0	104.0.0.0	252.0.0.0
5.0.0.0	255.0.0.0	127.0.0.0	255.0.0.0
10.0.0.0	255.0.0.0	169.254.0.0	255.255.0.0
14.0.0.0	255.0.0.0	172.16.0.0	255.240.0.0
23.0.0.0	255.0.0.0	176.0.0.0	254.0.0.0
27.0.0.0	255.0.0.0	179.0.0.0	255.0.0.0
31.0.0.0	255.0.0.0	181.0.0.0	255.0.0.0
36.0.0.0	254.0.0.0	185.0.0.0	255.0.0.0
39.0.0.0	255.0.0.0	192.0.2.0	255.255.255.0
42.0.0.0	255.0.0.0	192.168.0.0	255.255.0.0
46.0.0.0	255.0.0.0	198.18.0.0	255.254.0.0
49.0.0.0	255.0.0.0	223.0.0.0	255.0.0.0
50.0.0.0	255.0.0.0	224.0.0.0	224.0.0.0

2.2　访问控制列表基础

一个访问控制列表(Access Control List,ACL)由多条有顺序的规则(rule)组成,每一条规则都定义了一个匹配条件及相应的动作。包过滤防火墙通过引用相应的 ACL,使用 ACL 中的规则顺序对网络中的数据包进行分类匹配,并根据匹配规则中相应的动作允许或拒绝数据包的通过。根据引用 ACL 位置的不同,可以将 ACL 分为入站 ACL 和出站 ACL 两种,下面分别对其工作流程进行介绍。

2.2.1　入站 ACL 工作流程

默认情况下,路由器某个接口的入站(inbound)方向上没有应用 ACL,因此该接口 inbound 方向上的数据包将直接进入转发流程。如果在路由器某个接口的 inbound 方向上应用了 ACL,则该接口入站方向的数据包需要进行 ACL 的匹配。具体流程如下。

(1) 首先使用 ACL 定义的第一条规则去匹配数据包,如果匹配成功,则执行该规则定义的动作。如果动作为 Permit,则数据包通过并进入转发流程;如果动作为 Deny,则数据包被丢弃。

(2) 如果第一条规则匹配没有成功,则继续尝试匹配下一条 ACL 规则,直到匹配成功。

(3) 如果数据包没有匹配到任何一条规则,则执行 ACL 默认规则的动作。默认情况下,H3C 设备上的默认动作为 Permit,即允许数据包通过;Cisco 设备上的默认动作为 Deny,即禁止数据包通过。

H3C 设备上入站 ACL 的工作流程如图 2-2 所示。

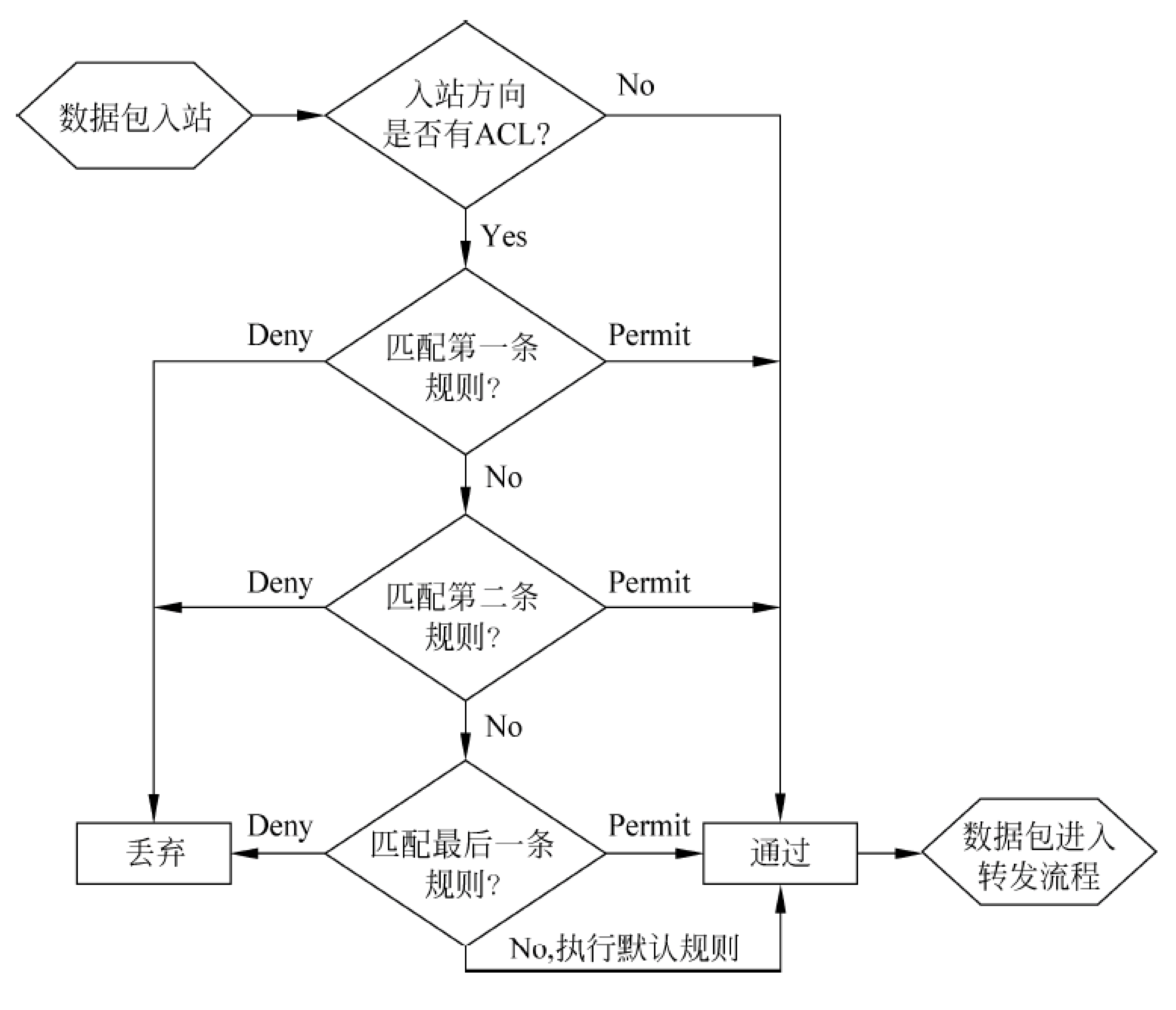


图 2-2　入站 ACL 工作流程

2.2.2 出站 ACL 工作流程

默认情况下,路由器某个接口的出站(outbound)方向上没有应用 ACL,因此该接口 outbound 方向上的数据包将直接从接口发出。如果在路由器某个接口的 outbound 方向上应用了 ACL,则该接口出站方向的数据包需要进行 ACL 的匹配。具体流程如下。

(1) 首先使用 ACL 的第一条规则去匹配数据包,如果匹配成功,则执行该规则定义的动作。如果动作为 Permit,则数据包直接从接口发出;如果动作为 Deny,则数据包被丢弃。

(2) 如果第一条规则匹配没有成功,则继续尝试匹配下一条 ACL 规则,直到匹配成功。

(3) 如果数据包没有匹配到任何一条规则,则执行 ACL 默认规则的动作。默认情况下,H3C 设备上的默认动作为 Permit,即允许数据包通过;Cisco 设备上的默认动作为 Deny,即禁止数据包通过。

H3C 设备上出站 ACL 的工作流程如图 2-3 所示。

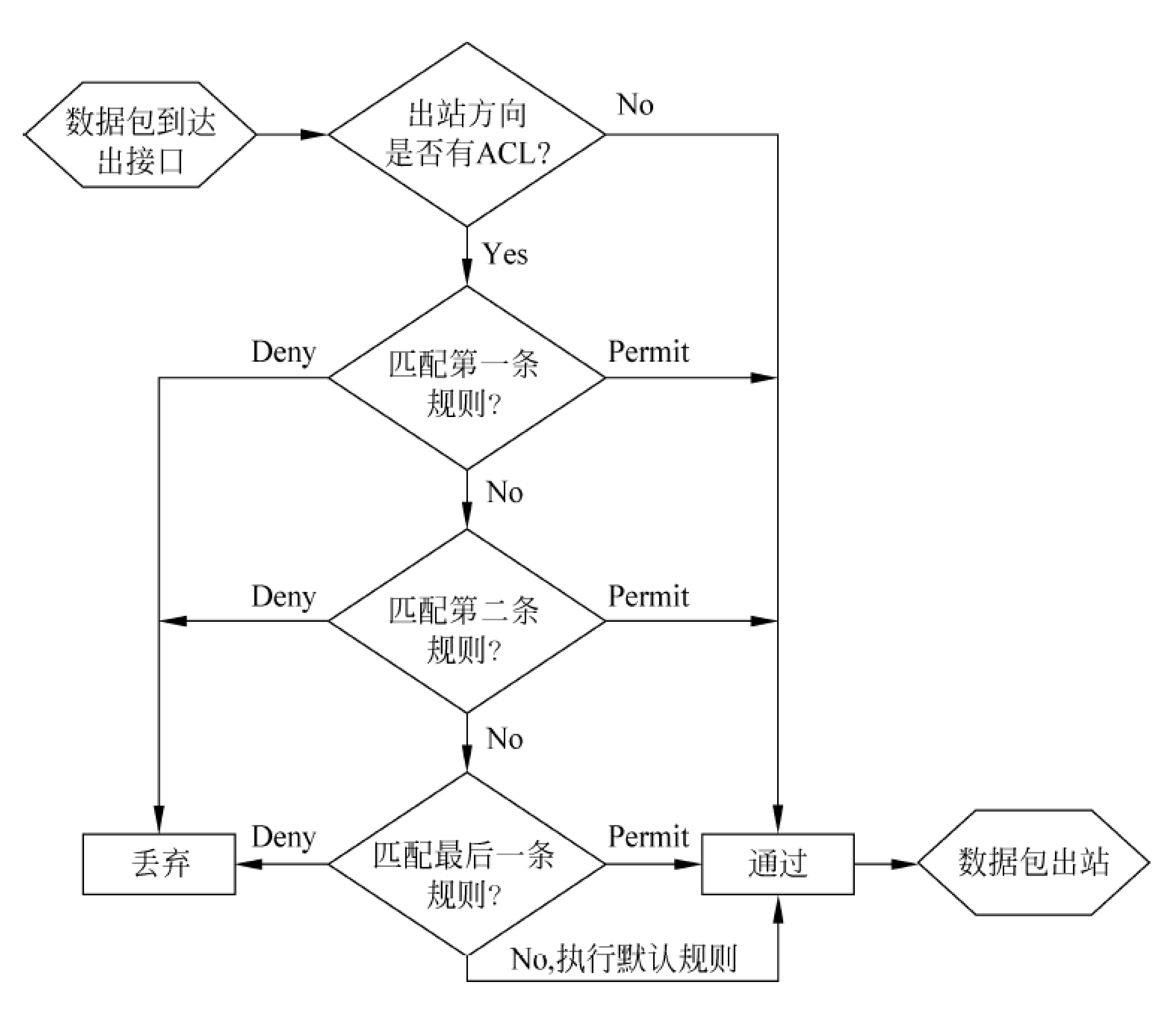


图 2-3 出站 ACL 工作流程

2.2.3 ACL 配置注意事项

在进行 ACL 的配置时需要注意以下 4 点。

(1) ACL 规则的顺序。由于 ACL 在默认情况下是按照规则的配置顺序进行数据包的匹配,只有在某一条规则匹配失败的情况下才会进行下一条规则的匹配,而一旦某一条规则匹配成功,则将直接执行相应的动作而不再匹配该条规则之后的规则,因此在写 ACL 时一定要正确配置多条规则之间的顺序。ACL 一般按照规则的约束性强弱对其进

行排序,将约束性最强的规则放置在 ACL 的顶部,而约束性最弱的规则放置在 ACL 的底部,以保证 ACL 能够被有效执行。

(2) 尽量避免使用 ACL 的默认规则。不同品牌的设备在对 ACL 默认规则的处理上不尽相同,例如,H3C 的设备上 ACL 默认规则的动作为 permit,而 Cisco 的设备上 ACL 默认规则的动作为 deny。而且默认规则的动作均可以通过命令来修改,这也造成了同一品牌的设备可能在默认规则上也会有所区别。因此为了保证 ACL 的健壮性和可移植性,一般应将所有规则显式地写出,而尽量避免使用 ACL 的默认规则。

(3) 在路由器接口的一个方向上只能应用一个 ACL,如果在已经应用了 ACL 某个接口的某个方向上再次应用一个 ACL,则最后应用的 ACL 将生效。

(4) ACL 只能对进入路由器的外部流量进行过滤,并不过滤应用 ACL 的路由器接口自身产生的流量。

2.2.4　通配符掩码

在 ACL 定义的规则中,匹配条件使用 IP 地址和通配符掩码来匹配特定地址段的数据包,其中通配符掩码用来定义匹配的地址范围,作用与子网掩码类似。与子网掩码相同的是,通配符掩码也是由 32 位的二进制数组成,可以表示为点分十进制形式;与子网掩码不同的是,在通配符掩码中如果某一位的值为 1,表示匹配条件中 IP 地址对应位可以忽略,如果某一位的值为 0,则表示匹配条件中 IP 地址对应位必须要匹配。一些网段的通配符掩码与子网掩码的比较如表 2-2 所示。

表 2-2　通配符掩码与子网掩码的比较

IP 网段	子 网 掩 码	通配符掩码
10.0.0.0/8	255.0.0.0	0.255.255.255
172.16.1.0/16	255.255.0.0	0.0.255.255
192.168.1.0/24	255.255.255.0	0.0.0.255
192.168.1.0/26	255.255.255.192	0.0.0.63

从表 2-2 中可以看出,ACL 的通配符掩码好像总是和子网掩码相反,这是因为 ACL 在进行匹配时往往也是以网段为单位,由于网络地址需要匹配,因此通配符掩码对应位需要取 0,主机位不需要匹配,因此通配符掩码对应位需要取 1。这样计算的结果总是和子网掩码求反的结果相同,因此通配符掩码在某些教材上又称为反掩码,事实上这种叫法并不准确。因为子网掩码中 1 或者 0 必须是连续的,而通配符掩码则没有这样的要求。

例如,如果一条规则要求匹配网段 202.207.120.0/24 中的所有主机号为偶数的主机,则匹配条件中 IP 地址为 202.207.120.0,通配符掩码为 0.0.0.254,用二进制表示通配符掩码为 00000000.00000000.00000000.11111110,即 IP 地址的最后一位必须匹配为 0。同理,如果一条规则要求匹配网段 202.207.120.0/24 中的所有主机号为奇数的主机,则匹配条件中 IP 地址为 202.207.120.1,通配符掩码为 0.0.0.254,即 IP 地址的最后一位必须匹配为 1。另一种情况是匹配多个不连续的网段,例如如果一条规则要求匹配 192.168.1.0/24 和 192.168.3.0/24 两个网段,则匹配条件中的 IP 地址为 192.168.1.0,通配符掩码为 0.0.2.255,用二进制表示通配符掩码为 00000000.00000000.00000010.

11111111,即IP地址中的第23位不需要进行匹配。

2.2.5 ACL的类型与编号

根据ACL规则中匹配条件的不同,ACL可以分为4种不同的类型,用不同范围的编号来进行区别。其中H3C设备上的ACL编号具体如表2-3所示。

表2-3 ACL类型与编号

ACL类型	编号范围
基本访问控制列表	2000～2999
高级访问控制列表	3000～3999
基于二层的访问控制列表	4000～4999
用户自定义的访问控制列表	5000～5999

基本ACL只能根据报文的源IP地址信息对数据包进行过滤。高级ACL可以根据报文中的源IP地址、目的IP地址、IP承载的协议类型、协议的特性等三、四层信息对数据包进行过滤。

基于二层的ACL可以根据报文的源MAC地址、目的MAC地址、VLAN优先级、二层协议类型等二层信息对数据包进行过滤。例如,可以使用基于二层的ACL来禁止以太帧头的VLAN标签中IEEE 802.1p(LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization)优先级为3的数据报文通过路由器,而允许其他数据报文通过。

用户自定义的ACL可以以报文的报文头、IP头等为基准,指定从第几个字节开始与掩码进行"与"操作,将从报文中提取出来的字符串和用户定义的字符串进行比较,从而对数据包进行过滤。例如,可以使用用户自定义的ACL来禁止ARP报文,即从以太帧头开始算起第13和14字节内容为0x0806的数据报文通过。

在Cisco设备上对应于基本访问控制列表,称为标准访问控制列表,编号范围为1～99和1300～1999;对应于高级访问控制列表,称为扩展访问控制列表,编号范围为100～199和2000～2699。另外,无论对于标准访问控制列表还是扩展访问控制列表,在Cisco设备上均可以使用命令访问控制列表的方式来进行配置,从而使用有意义的名字来代替访问控制列表的编号。

在本书中只对基本ACL和高级ACL进行介绍,关于基于二层的ACL和用户自定义的ACL的内容不再涉及,感兴趣的读者可以自行查阅相关资料。

在H3C设备上定义ACL时,给出ACL编号的同时也可以为ACL指定一个名称,便于ACL的记忆和维护。

2.2.6 ACL规则的匹配顺序

在H3C设备上,ACL支持两种不同的匹配顺序,分别是配置顺序(config)和自动排序(auto)。其中,配置顺序为按照规则配置的先后顺序进行数据包的匹配;自动排序则是按照规则深度优先的顺序进行数据包的匹配,即系统优先考虑约束性强的规则。系统默认匹配顺序为按配置顺序匹配,可以通过以下命令修改ACL的匹配顺序:

[H3C]acl number *acl-number* match-order {auto|config}

如果系统的匹配顺序为自动排序，则基本 ACL 和高级 ACL 遵循的匹配原则如下。

1. 基本 ACL 匹配原则

(1) 首先比较源 IP 地址范围，源 IP 地址范围小的规则优先。

(2) 如果源 IP 地址范围相同，则先配置的规则优先。

2. 高级 ACL 匹配原则

(1) 首先比较协议范围，指定了 IP 协议承载的协议类型的规则优先。

(2) 如果协议范围相同，则比较源 IP 地址的范围，源 IP 地址范围小的规则优先。

(3) 如果源 IP 地址范围相同，则比较目的 IP 地址的范围，目的 IP 地址范围小的规则优先。

(4) 如果目的 IP 地址范围也相同，则比较第四层 TCP/UDP 端口号的范围，端口号范围小的规则优先。

(5) 如果上述范围都相同，则先配置的规则优先。

在进行 ACL 的配置时，一定要确定该 ACL 使用的匹配顺序。对于同一个 ACL，如果使用的匹配顺序不同，很可能会导致不同的执行结果。

2.3　基本访问控制列表

由于基本 ACL 只能根据报文的源 IP 地址信息对数据包进行过滤，因此一般适用于过滤从特定网络来的数据流量等相对简单的情况。按照基本 ACL 应用位置的不同，可以将其分为应用在接口上的基本 ACL 和应用在虚拟终端连接(Virtual Type Terminal，VTY)上的基本 ACL。

2.3.1　应用在接口上的基本 ACL

1. H3C 设备的配置

在 H3C 设备上配置应用在接口上的基本 ACL 涉及的命令如下。

(1) 启动防火墙功能。默认情况下路由器的防火墙功能是关闭的，必须通过 firewall enable 命令将其启动。

```
[H3C]firewall enable
```

(2) 定义一个基本 ACL，其中 acl-number 的取值范围为 2000～2999。

[H3C]acl number *acl-number* name *name*

(3) 在 ACL 配置视图下，定义该 ACL 的规则。

[H3C-acl-basic-2000] rule [*rule-id*] {deny | permit} [source {*sour-addr sour-wildcard* | any} | fragment | logging | time-range *time-name*]

其中各个参数的解释如下。

rule-id：规则 ID，在一个 ACL 下可以定义多个规则，按照规则 ID 从小到大的顺序排列。默认情况下规则 ID 的步长为 5，即相邻规则之间的编号之差为 5。使用较大的步

长设定能够方便用户在已有规则之间插入新的规则,从而方便对 ACL 的管理和维护。

deny|permit:相应规则的动作,deny 表示丢弃符合匹配条件的报文;permit 表示允许符合匹配条件的报文。

source {*sour-addr sour-wildcard* | any}:指定相应规则的源 IP 地址信息。*sour-addr* 表示报文的源 IP 地址;*sour-wildcard* 表示通配符掩码;any 表示匹配任意 IP 地址。

fragment:分片信息,用来定义相应规则仅对非首片分片报文有效,而对非分片报文和首片分片报文无效。默认情况下,ACL 对于非分片报文和分片报文均有效。

logging:对符合匹配条件的报文记录日志信息。

time-range *time-name*:指定规则生效的时间段。具体在 2.4 节中进行详细介绍。

(4) 将 ACL 应用到特定接口的特定方向上。

```
[H3C-Ethernet0/0]firewall packet-filter {acl-number|name acl-name} {inbound|outbound}
```

假设存在如图 2-4 所示的网络,网络联通性已经配置完成。要求配置基本 ACL 以禁止 10.1.1.0/24 网段的主机访问网段 13.1.1.0/24,但是允许其他所有网段之间的互访。

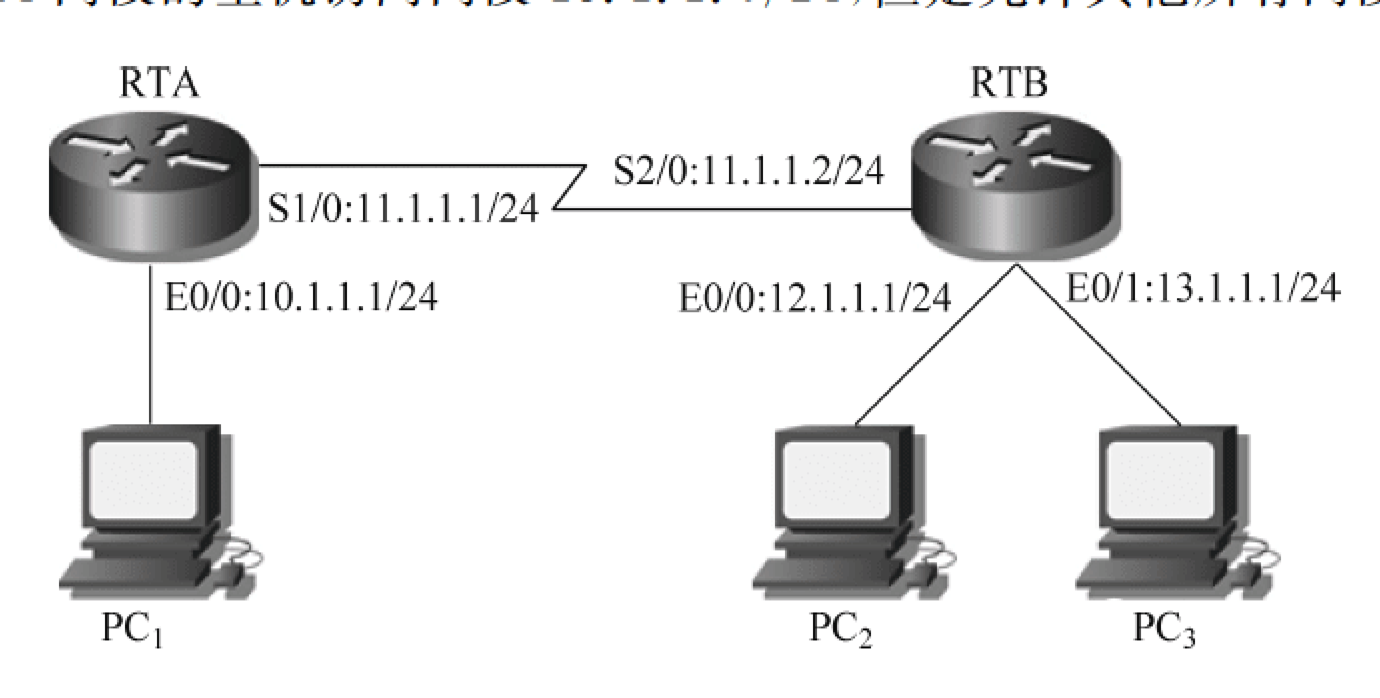


图 2-4　基本 ACL 的配置

现对任务分析如下。

(1) 由于基本 ACL 只能根据报文的源 IP 地址信息对数据包进行过滤,因此要满足禁止 10.1.1.0/24 网段的主机访问网段 13.1.1.0/24 的要求,定义的 ACL 规则中的源 IP 地址应为 10.1.1.0,通配符掩码应为 0.0.0.255。

(2) 该基本 ACL 只能应用在 RTB 接口 Ethernet 0/1 的 outbound 方向上。如果应用在其他位置,则有可能将从 10.1.1.0/24 网段去往其他网段的正常流量过滤掉。例如,将 ACL 应用到路由器 RTA 的 Ethernet 0/0 的 inbound 方向上,则将导致 10.1.1.0/24 网段无法访问任何其他网段。一般而言,对于 ACL 的应用位置原则是在不影响其他合法流量的前提下,尽可能使其靠近被拒绝的源。但是实际上基本 ACL 都需要应用在离目的地比较近的位置,否则总是会影响到正常流量的转发。

具体的配置命令如下:

```
[RTB]firewall enable
[RTB]acl number 2000
[RTB-acl-basic-2000]rule deny source 10.1.1.0 0.0.0.255
```

```
[RTB-acl-basic-2000]rule permit
[RTB-acl-basic-2000]quit
[RTB]interface Ethernet 0/1
[RTB-Ethernet0/1]firewall packet-filter 2000 outbound
```

需要注意的是，一般在配置 ACL 的时候，最后一条规则总是显式地给出允许所有或拒绝所有，而避免使用默认规则，以保证 ACL 的可移植性和健壮性。

配置完成后，在路由器 RTB 上执行 display acl all 命令显示结果如下：

```
[RTB]display acl all
Basic ACL 2000, named -none-, 2 rules,
ACL's step is 5
rule 0 deny source 10.1.1.0 0.0.0.255 (4 times matched)
rule 5 permit (31 times matched)
```

从上面显示的结果可以看出，在路由器 RTB 上配置了基本 ACL，编号为 2000，包含两条规则，ACL 的规则 ID 步长为 5，其中两条规则分别有 4 次命中和 31 次命中。

在路由器 RTB 上执行 display firewall-statistics all 命令显示结果如下：

```
[RTB]display firewall-statistics all
  Firewall is enable, default filtering method is 'permit'.

  Interface: Ethernet0/1
  Out-bound Policy: acl 2000
  Fragments matched normally
  From 2011-11-03 15:34:02 to 2011-11-03 15:51:37
     35 packets, 3188 bytes, 89% permitted,
     4 packets, 240 bytes, 11% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 35 packets, 3188 bytes, 89% permitted,
  Totally 4 packets, 240 bytes, 11% denied.
```

从上面显示的结果可以看出，在路由器 RTB 上防火墙处于开启状态，默认的过滤规则是允许，在接口 Ethernet 0/1 的出站方向上应用了 ACL 2000，以及对数据报文过滤的详细统计信息。

在用户视图下使用命令 reset firewall-statistics all 和 reset acl counter all，可以清空防火墙统计信息和 ACL 的报文命中信息。

此时在 PC_1 上使用 ping 命令进行测试会发现 PC_1 无法访问 PC_3，但可以访问 PC_2，从而验证了该基本 ACL 应用正确。

2. Cisco 设备的配置

在 Cisco 设备上配置应用在接口上的标准 ACL 涉及的命令如下。

(1) 定义一个标准 ACL，其中 access-list-number 的取值范围为 1～99 和 1300～1999。

Router(config)#access-list *access-list-number* {permit|deny} *source* [*source-wildcard*] [log]

首先，在 Cisco 设备上默认防火墙功能处于启动状态，因此在配置 ACL 之前不需要

使用专门的命令来启动防火墙功能；其次，在Cisco设备上ACL的配置是在全局配置模式下进行的，通过参数access-list-number来判断多个ACL语句是否属于同一个ACL。

(2) 将ACL应用到特定接口的特定方向上。

```
Router(config-if)#ip access-group access-list-number {in|out}
```

在Cisco设备上也可以使用命名ACL来配置标准ACL。命名标准ACL的配置命令如下。

```
Router(config)#ip access-list standard name
Router(config-std-nacl)# {permit|deny} source [source-wildcard] [log]
```

在此依然对图2-4所示的网络进行标准ACL的配置，具体的配置命令如下。

```
RTB(config)#ip access-list standard abc
RTB(config-std-nacl)#deny 10.1.1.0 0.0.0.255
RTB(config-std-nacl)#permit any
RTB(config-std-nacl)#exit
RTB(config)#interface FastEthernet 0/1
RTB(config-if)#ip access-group abc out
```

配置完成后，在路由器RTB上执行show access-lists命令显示结果如下。

```
RTB# show access-lists
Standard IP access list abc
    deny    10.1.1.0, wildcard bits 0.0.0.255 (8 matches)
    permit  any (4 matches)
```

从上面的显示结果可以看出，在路由器RTB上配置了命名标准ACL，名称为abc，包含两条规则，分别有8次命中和4次命中。

此时在PC_1上使用ping命令进行测试会发现PC_1无法访问PC_3，但可以访问PC_2，从而验证了该标准ACL应用正确。

2.3.2 应用在VTY上的基本ACL

1. H3C设备的配置

在H3C设备上配置应用在VTY上的基本ACL和配置应用在接口上的基本ACL所涉及的命令基本相同，唯一的区别是第4步将基本ACL应用在VTY上的命令，具体如下。

```
[H3C-ui-vty0-4]acl acl-number {inbound|outbound}
```

在这里依然使用图2-4所示的网络，假设路由器RTB的管理接口为LoopBack 0，管理地址为1.1.1.1/32，并在RIPv2协议中进行发布。在路由器RTB上开启虚拟终端连接服务，设置其验证方式为密码验证方式，密码为123，登录运行级别为管理级。具体配置命令如下。

```
[RTB]interface LoopBack 0
[RTB-LoopBack0]ip address 1.1.1.1 32
```

```
[RTB-LoopBack0]quit
[RTB]rip
[RTB-rip-1]version 2
[RTB-rip-1]undo summary
[RTB-rip-1]network 1.0.0.0
[RTB-rip-1]quit
[RTB]telnet server enable
[RTB]user-interface vty 0 4
[RTB-ui-vty0-4]authentication-mode password
[RTB-ui-vty0-4]set authentication password simple 123
[RTB-ui-vty0-4]user privilege level 3
```

注意：本部分涉及的环回接口、RIPv2 以及虚拟终端连接的相关知识在“网络集成技术”课程中进行讲解，在此只使用其命令，具体内容不做介绍。

配置完成后，在 PC_1、PC_2 和 PC_3 上均可以通过 Telnet 方式连接到路由器 RTB 上，具体如下。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>telnet 1.1.1.1

****************************************************************************
* Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                   *
****************************************************************************
Login authentication
Password:
<RTB>system-view
System View: return to User View with Ctrl+Z.
[RTB]
```

假设 PC_2 的 IP 地址为 12.1.1.2/24，要求配置应用在 VTY 上的基本 ACL，以禁止 PC_2 通过 Telnet 方式连接到路由器 RTB 上，而允许其他主机 Telnet 到路由器 RTB 上，具体的配置命令如下。

```
[RTB]firewall enable
[RTB]acl number 2001
[RTB-acl-basic-2001]rule deny source 12.1.1.2 0
[RTB-acl-basic-2001]rule permit
[RTB-acl-basic-2001]quit
[RTB]user-interface vty 0 4
[RTB-ui-vty0-4]acl 2001 inbound
```

需要注意的是，与应用在接口上的基本 ACL 不同，对于应用在 VTY 上的基本 ACL 其默认规则为拒绝所有流量，也就是说如果在上面的 ACL 中没有配置规则 rule permit，则所有的 PC 均无法通过 Telnet 的方式连接到路由器 RTB 上。

配置完成后，在 PC_2 上通过 Telnet 方式连接路由器 RTB 显示结果如下。

```
C:\Documents and Settings\Administrator>telnet 1.1.1.1
%connection closed by remote host!
失去了跟主机的连接.
```

而在 PC_1 和 PC_3 上均可以通过 Telnet 方式连接到路由器 RTB 上,从而验证了该基本 ACL 应用正确。

2. Cisco 设备的配置

在 Cisco 设备上配置应用在 VTY 上的标准 ACL 和配置应用在接口上的标准 ACL 所涉及的命令基本相同,唯一的区别是第 2 步将基本 ACL 应用在 VTY 上的命令,具体如下。

```
Router(config)#line vty 0 4
Router(config-line)#access-class {access-list-number|access-list-name} {in|out}
```

在此,配置要求与上面 H3C 设备的配置要求相同,具体的配置命令如下。

```
RTB(config)#ip access-list standard tel
RTB(config-std-nacl)#deny host 12.1.1.2
RTB(config-std-nacl)#permit any
RTB(config-std-nacl)#exit
RTB(config)#line vty 0 4
RTB(config-line)#access-class tel in
```

配置完成后,在 PC_1 和 PC_3 上均可以通过 Telnet 方式连接到路由器 RTB 上,PC_2 则无法 Telnet 到路由器 RTB 上,从而验证了该基本 ACL 应用正确。

2.4 高级访问控制列表

2.4.1 高级 ACL 的基础应用

高级 ACL 可以根据报文中的源 IP 地址、目的 IP 地址、IP 承载的协议类型、协议的特性等三、四层信息对数据包进行过滤,因此比较适用于过滤某些网络中的特定应用以及过滤精确的数据流。

1. H3C 设备的配置

在 H3C 设备上配置高级 ACL 涉及的命令如下。

(1) 启动防火墙功能。默认情况下路由器的防火墙功能是关闭的,必须通过 firewall enable 命令将其启动。

```
[H3C]firewall enable
```

(2) 定义一个高级 ACL。其中 *acl-number* 的取值范围为 3000～3999。

```
[H3C]acl number acl-number name name
```

(3) 在 ACL 配置视图下,定义该 ACL 的规则。

```
[H3C-acl-adv-3000]rule [rule-id] {deny|permit} protocol [source {sour-addr sour-wildcard|any}
|source-port operator port1 [port2]|destination {dest-addr dest-wildcard|any}|destination-port
```

*operator port*1 [*port*2] established | *icmp-type* {*icmp-type icmp-code* | *icmp-message*} | fragment | logging | time-range *time-name*]

其中部分参数的解释如下。

protocol：IP 承载的协议类型。用数字表示时，取值范围为 0～255；用名字表示时，可以选取 gre(47)、icmp(1)、igmp(2)、ip、ipinip(4)、ospf(89)、tcp(6)、udp(17)。如果某条规则定义的协议类型为 ip，则该规则覆盖所有的其他协议数据报文。

operator：端口操作符。在协议类型为 TCP 或 UDP 时使用的参数，可以取值 lt(小于)、gt(大于)、eq(等于)、neq(不等于)或者 range(在范围内，包括边界值)。其中只有 range 需要两个端口号作为操作数，其他的取值只需要一个端口号作为操作数。

*port*1、*port*2：TCP 或 UDP 的端口号，取值范围为 0～65535，也可以用文字表示。

established：TCP 连接建立标识，用于匹配一个已建立的 TCP 连接。如果 TCP 数据报文中的响应位 ACK 或重置连接位 RST 等控制位被置位，则匹配；如果是要求建立 TCP 连接的初始数据报文，则不匹配。

icmp-type {*icmp-type icmp-code* | *icmp-message*}：ICMP 报文的消息类型和消息码信息，在协议类型为 ICMP 时使用的参数。其中，*icmp-type* 是指 ICMP 的消息类型，取值范围为 0～255；*icmp-code* 是指 ICMP 的消息码，取值范围为 0～255；*icmp-message* 是指 ICMP 消息的名称。一般在高级 ACL 中比较常用到的两种 ICMP 消息为 ICMP echo 消息和 ICMP echo-reply 消息。

(4) 将 ACL 应用到特定接口的特定方向上。

```
[H3C-Ethernet0/0]firewall packet-filter {acl-number | name acl-name} {inbound | outbound}
```

在这里依然使用图 2-4 所示的网络拓扑，要求使用高级 ACL 实现相同的流量控制，具体的配置命令如下。

```
[RTA]firewall enable
[RTA]acl number 3000
[RTA-acl-adv-3000]rule deny ip source 10.1.1.0 0.0.0.255 destination 13.1.1.0 0.0.0.255
[RTA-acl-adv-3000]rule permit ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/0
[RTA-Ethernet0/0]firewall packet-filter 3000 inbound
```

由于高级 ACL 可以实现对流量的精确匹配，因此一般应用在靠近被过滤源的接口上，以尽早阻止不必要的流量进入网络。在这里将高级 ACL 应用在路由器 RTA 接口 Ethernet 0/0 的 inbound 方向上。

此时在 PC_1 上使用 ping 命令进行测试会发现 PC_1 无法访问 PC_3，但可以访问 PC_2，从而证明了该高级 ACL 应用正确。

2. Cisco 设备的配置

在 Cisco 设备上配置扩展 ACL 涉及的命令如下。

(1) 定义一个扩展 ACL。其中 access-list-number 的取值范围为 100～199 和 2000～2699。

```
Router(config)# access-list access-list-number {permit|deny} protocol source source-wildcard
[operator [port]] destination destination-wildcard [operator [port]] [established] [fragment|
log| time-range time-name]
```

首先,在Cisco设备上默认防火墙功能处于启动状态,因此在配置ACL之前不需要使用专门的命令来启动防火墙功能;其次,在Cisco设备上ACL的配置是在全局配置模式下进行的,通过参数access-list-number来判断多个ACL语句是否属于同一个ACL。

(2) 将ACL应用到特定接口的特定方向上。

```
Router(config-if)#ip access-group access-list-number {in|out}
```

在Cisco设备上也可以使用命名ACL来配置扩展ACL,配置命令如下。

```
Router(config)#ip access-list extended name
Router(config-ext-nacl)# {permit|deny} protocol source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]] [established] [fragment|log| time-range time-
name]
```

在这里依然使用图2-4所示的网络拓扑,要求使用扩展ACL实现相同的流量控制,具体的配置命令如下。

```
RTA(config)#ip access-list extended abc
RTA(config-ext-nacl)#deny ip 10.1.1.0 0.0.0.255 13.1.1.0 0.0.0.255
RTA(config-ext-nacl)#permit ip any any
RTA(config-ext-nacl)#exit
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip access-group abc in
```

此时在PC_1上使用ping命令进行测试会发现PC_1无法访问PC_3,但可以访问PC_2,从而证明了该扩展ACL应用正确。

2.4.2 高级ACL的典型应用

高级ACL的典型应用是在一个局域网络的出口路由器上。为确保内部网络的安全,往往需要在出口路由器与外部网络连接接口的inbound方向上应用高级ACL,以实现对外部网络的恶意流量进行过滤的目的。

假设存在如图2-5所示的网络。

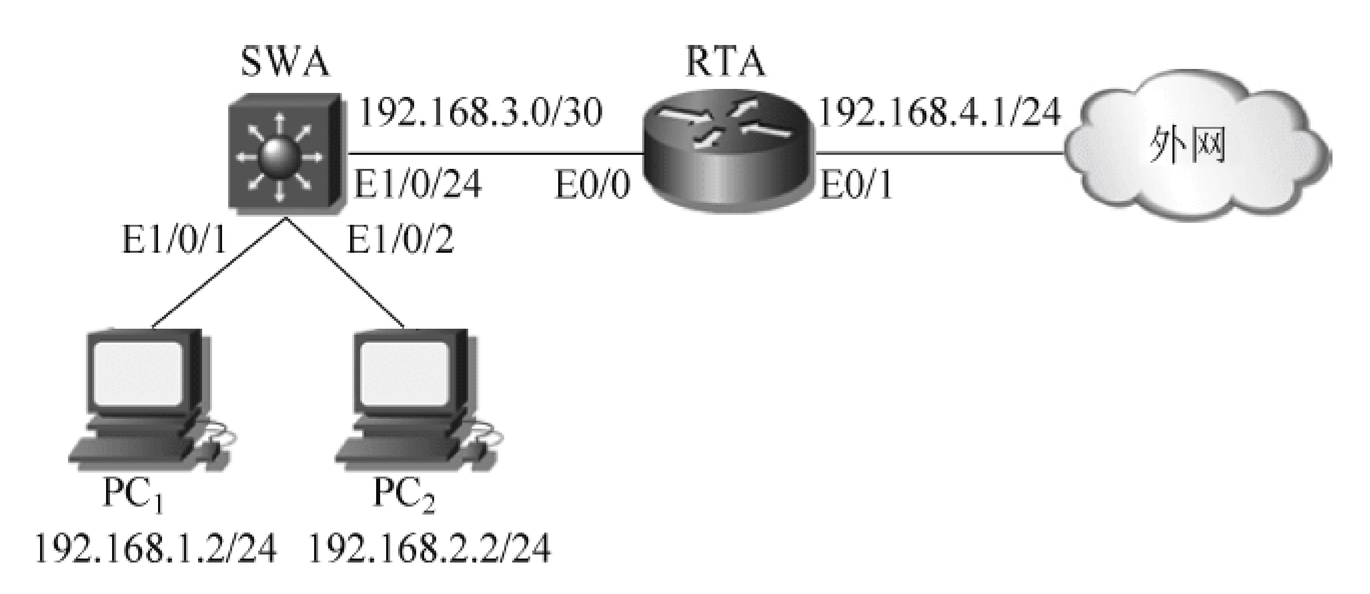


图2-5 高级ACL的典型应用

其中,要求内部网络可以随意访问外部网络,而外部网络访问内部网络受到以下限制。

（1）外部网络可以访问内网主机 192.168.1.2 上的 HTTP 服务。

（2）禁止外部网络访问其他任何关于内网基于 TCP 的服务。

（3）禁止外部网络主动 ping 内部网络主机。

（4）允许其他类型的访问。

现对任务分析如下。

（1）在应用位置上,出于保护内部网络安全的考虑,一般都会将 ACL 应用在出口路由器与外部网络连接接口的 inbound 方向上,即路由器 RTA E0/1 接口的 inbound 方向上。

（2）对于第二条限制要求"禁止外部网络访问其他任何关于内网基于 TCP 的服务"实际上可以分解为两条：首先允许内部网络访问外部网络的响应流量,即只允许 ACK 或者 RST 标志位被置位的 TCP 流量进入内部网络；然后拒绝其他所有来自于外部网络的 TCP 流量。

（3）按照约束性的强弱,第一条限制要求产生的规则一定排在第二条限制要求产生的规则之前,否则会导致访问控制的错误；但是第三条限制要求产生的规则可以放置在第一条限制要求产生的规则之前,也可以放置在第二条限制要求产生的规则之后,因为 ICMP 协议和 TCP 协议之间没有任何约束性关系。

（4）第四条限制要求实际上是要求显式地写出默认规则,以保证 ACL 的可移植性和健壮性。

H3C 设备上具体的配置命令如下。

```
[RTA]firewall enable
[RTA]acl number 3000
[RTA-acl-adv-3000]rule permit tcp destination 192.168.1.2 0 destination-port eq 80
[RTA-acl-adv-3000]rule permit tcp established
[RTA-acl-adv-3000]rule deny tcp
[RTA-acl-adv-3000]rule deny icmp icmp-type echo
[RTA-acl-adv-3000]rule permit ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall packet-filter 3000 inbound
```

Cisco 设备上具体的配置命令如下。

```
RTA(config)#ip access-list extended abc
RTA(config-ext-nacl)#permit tcp any host 192.168.1.2 eq 80
RTA(config-ext-nacl)#permit tcp any any established
RTA(config-ext-nacl)#deny tcp any any
RTA(config-ext-nacl)#deny icmp any any echo
RTA(config-ext-nacl)#permit ip any any
RTA(config-ext-nacl)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip access-group abc in
```

配置完成后,可以通过ping命令和IE浏览器对结果进行测试,并使用命令display acl all或者show access-lists查看具体的规则匹配情况。

2.4.3 高级ACL控制FTP流量的应用

在2.4.2小节的例子中,只是允许外部网络可以访问内网主机192.168.1.2上的HTTP服务,假设内网主机192.168.1.2还需要向外部网络提供FTP服务,则需要在ACL中增加相应的规则。H3C设备上的配置具体如下。

```
[RTA]acl number 3000
[RTA-acl-adv-3000]rule 2 permit tcp destination 192.168.1.2 0 destination-port eq 21
[RTA-acl-adv-3000]rule 3 permit tcp destination 192.168.1.2 0 destination-port eq 20
```

需要注意的是,按照约束性的强弱,新增加的两条规则需要放置在原第二条规则之前。增加规则后,ACL 3000的具体配置如下。

```
[RTA-acl-adv-3000]display this
#
acl number 3000
  rule 0 permit tcp destination 192.168.1.2 0 destination-port eq www
  rule 2 permit tcp destination 192.168.1.2 0 destination-port eq ftp
  rule 3 permit tcp destination 192.168.1.2 0 destination-port eq ftp-data
  rule 5 permit tcp established
  rule 10 deny tcp
  rule 15 deny icmp icmp-type echo
  rule 20 permit ip
#
return
```

Cisco设备上的配置与H3C设备的配置类似,区别在于在Cisco设备上需要首先将后4条规则删除掉,然后再配置允许FTP的规则,并重新配置后4条规则,具体在此不再赘述。

配置完成后,按照正常推理,在外部网络主机上应该可以连接内网主机192.168.1.2上的FTP服务,但是实际情况是根本无法连接。在路由器RTA上使用display acl 3000命令查看ACL 3000的报文匹配情况如下。

```
[RTA]display acl 3000
Advanced ACL  3000, named -none-, 7 rules
ACL's step is 5
  rule 0 permit tcp destination 192.168.1.2 0 destination-port eq www (2 times matched)
  rule 2 permit tcp destination 192.168.1.2 0 destination-port eq ftp (12 times matched)
  rule 3 permit tcp destination 192.168.1.2 0 destination-port eq ftp-data
  rule 5 permit tcp established (5 times matched)
  rule 10 deny tcp (12 times matched)
  rule 15 deny icmp icmp-type echo (1 times matched)
  rule 20 permit ip (22 times matched)
```

从上面显示的结果可以看出,第3条规则没有匹配任何流量,也就是说外部网络主机与内网主机192.168.1.2上的FTP数据端口(TCP的20端口)之间没有进行任何数据

传输。之所以会出现这样的情况，实际上和 FTP 的工作模式有关。按照连接模式的差异，可以将 FTP 分为主动模式和被动模式两种。

1. 主动模式

主动模式(Port Mode)是 FTP 的传统连接模式，FTP 在主动模式下的连接过程如下。

(1) FTP 客户端开启一个大于 1024 的随机端口 N 连接到 FTP 服务器的命令端口 21 上。

(2) FTP 客户端开始监听自己的 N＋1 端口，并向 FTP 服务器的命令端口发送"PORT N+1"命令来通知 FTP 服务器自己已经在端口 N+1 上做好了接收数据的准备。

(3) FTP 服务器接收到命令后，打开其 20 端口作为数据端口与 FTP 客户端的 N+1 端口建立连接，进行数据传输。

可见在主动模式中，数据连接是由 FTP 服务器主动发起的，FTP 服务器端的数据端口为 20 端口。

2. 被动模式

被动模式(Passive Mode)出现相对较晚，由于主动模式需要 FTP 客户端主机打开一个数据端口进行监听，而这个端口很有可能会被本机的一些安全策略(如本机的软件防火墙)阻塞掉，因此开发了 FTP 的被动连接模式。FTP 在被动模式下的连接过程如下。

(1) FTP 客户端开启一个大于 1024 的随机端口 N 连接到 FTP 服务器的命令端口 21 上。

(2) FTP 客户端开启自己的 N+1 端口，并向 FTP 服务器的命令端口发送 PASV 命令来通知 FTP 服务器自己工作在被动模式。

(3) FTP 服务器接收到命令后，会开启一个大于 1024 的随机端口 X 进行监听，并向 FTP 客户端的命令端口发送"PORT X"命令来通知 FTP 客户端自己已经在端口 X 上做好接收数据的准备。

(4) FTP 客户端接收到命令后，通过自己的 N+1 号端口与 FTP 服务器的数据端口 X 建立连接，进行数据的传输。

可见在被动模式中，数据连接是由 FTP 客户端主动发起的，FTP 服务器端的数据端口为大于 1024 的随机端口，而不是 20 端口。在默认情况下，IE 以及常见的一些 FTP 客户端工具都使用被动模式进行连接。

正是因为 FTP 客户端的 IE 工作在被动模式，因此在建立数据连接的时候 FTP 客户端会主动向 FTP 服务器的数据端口 X 发起连接请求，而这些请求都会因为匹配了规则 rule deny tcp 而被拒绝，从而导致外部网络主机上无法连接内网主机 192.168.1.2 上的 FTP 服务。解决的方法就是采用主动模式进行 FTP 连接。具体的操作方法是在 IE 的菜单栏中选择"工具"→"Internet 选项"→"高级"，然后找到"使用被动 FTP(用于防火墙和 DSL 调制解调器的兼容)"复选框，取消选中即可，如图 2-6 所示。

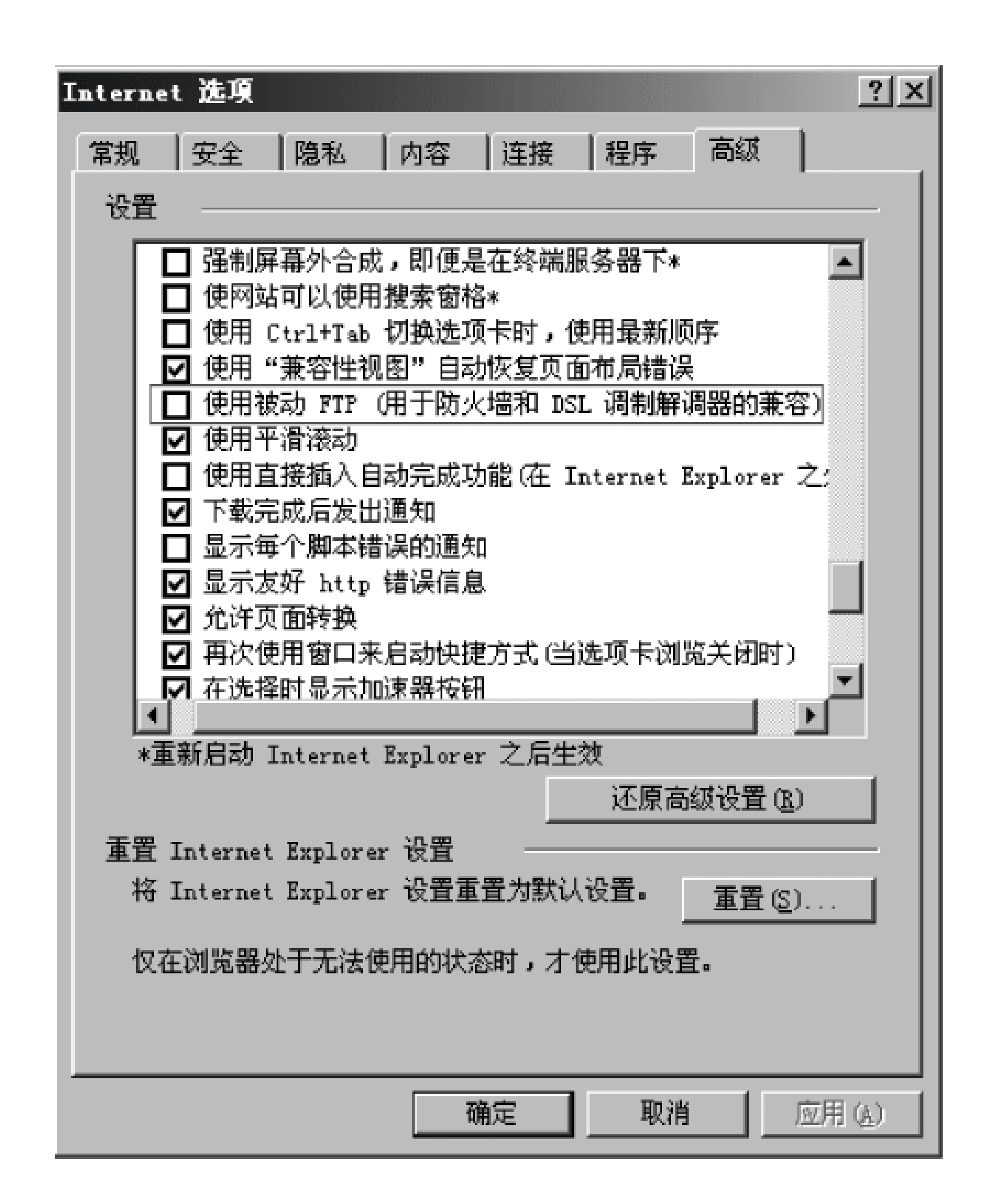


图 2-6 设置 FTP 为主动模式

设置完成后,在外部网络主机上使用 IE 即可连接到内网主机 192.168.1.2 上的 FTP 服务。此时,在路由器 RTA 上再次使用 display acl 3000 命令查看 ACL 3000 的报文匹配情况如下。

```
[RTA]display acl 3000
Advanced ACL 3000, named -none-, 7 rules
ACL's step is 5
  rule 0 permit tcp destination 192.168.1.2 0 destination-port eq www (2 times matched)
  rule 2 permit tcp destination 192.168.1.2 0 destination-port eq ftp (26 times matched)
  rule 3 permit tcp destination 192.168.1.2 0 destination-port eq ftp-data (4 times matched)
  rule 5 permit tcp established (5 times matched)
  rule 10 deny tcp (25 times matched)
  rule 15 deny icmp icmp-type echo (1 times matched)
  rule 20 permit ip (79 times matched)
```

从上面显示的结果可以看出,第 3 条规则有相匹配的流量,这也说明在主动模式下 FTP 服务器端的数据端口为 20 端口。

关于主动模式和被动模式孰优孰劣并没有定论,显然主动模式有利于 FTP 服务器端的安全,但对 FTP 客户端的安全不利,因为需要 FTP 客户端开启某个高位端口进行监听;而被动模式有利于 FTP 客户端的安全,但对 FTP 服务器端的安全不利,因为需要 FTP 服务器端开启某个高位端口进行监听。具体采用哪种连接模式,还是要根据具体的网络应用和网络安全的需求来决定。

另外,高级 ACL 也可以应用在虚拟终端连接(Virtual Type Terminal,VTY)上,应用命令与基本 ACL 在 VTY 上的应用相同,在此不再进行介绍。

2.5　定时访问控制列表

首先需要说明的是，定时 ACL 并不是一种单独的 ACL 类别，在基础 ACL 和高级 ACL 中均可以通过引用时间段来组成定时访问控制列表。创建定时访问控制列表实际上分为两个步骤：首先定义一个时间段；然后在 ACL 的规则中引用相应的时间段。

在 H3C 设备上定义时间段的命令如下。

[H3C] time-range *time-range-name* { *start-time to end-time days* [from *time1 date1*] [to *time2 date2*] | from *time1 date1* [to *time2 date2*] | to *time2 date2* }

通过定义时间段的命令实际上可以定义两种不同类型的时间段：周期时间段和绝对时间段。周期时间段是以星期为单位进行循环；而绝对时间段是指某一段具体的日期。

其中命令中涉及的参数解释如下。

time-range-name：时间段的名称，要求最大为 32 个字符。每一个时间段由唯一的名称来标识。

start-time to end-time days：本部分参数用来定义周期时间段。其中，*start-time* 和 *end-time* 分别用来定义该时间段的起始时间和结束时间，时间格式为 hh:mm；*days* 用来定义该时间段在星期几生效。*days* 参数的具体取值及其含义如表 2-4 所示。

表 2-4　*days* 参数的取值及含义

取　值	含　义	取　值	含　义
Mon	星期一	Tue	星期二
Wed	星期三	Thu	星期四
Fri	星期五	Sat	星期六
Sun	星期日	daily	每周的任何一天
working-day	星期一至星期五	off-day	星期六和星期日
<0-6>	0 代表星期日，1-6 分别代表星期一到星期六		

time1 date1：定义绝对时间段的起始时间和起始日期。*time1* 为起始时间，格式为 hh:mm；*date1* 为起始日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日）。

time2 date2：定义绝对时间段的结束时间和结束日期。格式要求与起始时间和起始日期相同。

在 Cisco 设备上定义时间段的命令如下。

Router (config)# time-range *time-range-name*
Router(config-time-range)# absolute [start *time1 date1*] [end *time2 date2*]
Router (config-time-range)# periodic *days start-time* to *end-time*

其中，absolute 用来定义绝对时间段，而 periodic 用来定义相对时间段。在指定相对时间段时，参数 *days* 的取值与 H3C 设备上类似，区别在于 Cisco 设备上的某一天使用其英文的全称，例如星期一为 Monday，工作日使用 weekdays 表示，休息日使用 weekend

表示。

在定义时间段时需要注意以下两个问题。

(1) 在同一个时间段名字下可以配置多个时间段。在同一个时间段名字下配置的多个周期时间段之间是“或”的关系;多个绝对时间段之间是“或”的关系;而周期时间段和绝对时间段之间是“与”的关系。

(2) 在配置绝对时间段时,如果不配置开始日期,时间段就是从系统可表示的最早时间(即1970年1月1日0点0分)起到结束日期为止;如果不配置结束日期,时间段就是从配置生效之日起到系统可以表示的最晚时间(即2100年12月31日24点0分)为止。

假设在H3C设备上定义一个时间段为每周工作日的8:00到18:00,则配置命令为。

```
[H3C]time-range work 8:00 to 18:00 working-day
```

配置完成后,通过display time-range all命令查看所定义的时间段情况如下。

```
[H3C]display time-range all
Current time is 16:58:23 11/4/2011 Friday

Time-range : work (Active )
  08:00 to 18:00 working-day
```

从显示的结果可以看出,定义了一个名字为work时间段,并且该时间段处于激活状态,即当前系统时间处于定义的时间段之内。

在此依然使用图2-5所示的网络,其中内部网络可以随意访问外部网络,而外部网络访问内部网络受到的限制变更为以下要求。

(1) 外部网络仅在星期六和星期日的8:00—12:00之间可以访问内网主机192.168.1.2上的HTTP服务。

(2) 禁止外部网络访问其他任何关于内网的基于TCP的服务。

(3) 禁止外部网络在主动ping内部网络主机。

(4) 允许其他类型的访问。

则H3C设备上具体的配置命令如下。

```
[RTA]firewall enable
[RTA]time-range visit 8:00 to 12:00 off-day
[RTA]acl number 3000
[RTA-acl-adv-3000]rule permit tcp destination 192.168.1.2 0 destination-port eq 80 time-range visit
[RTA-acl-adv-3000]rule permit tcp established
[RTA-acl-adv-3000]rule deny tcp
[RTA-acl-adv-3000]rule deny icmp icmp-type echo
[RTA-acl-adv-3000]rule permit ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall packet-filter 3000 inbound
```

配置完成后,在路由器RTA上执行display acl 3000显示结果如下。

```
[RTA]display acl all
Advanced ACL  3000, named -none-, 5 rules,
ACL's step is 5
 rule 0 permit tcp destination 192.168.1.2 0 destination-port eq www time-range visit (Inactive)
 rule 5 permit tcp established
 rule 10 deny tcp
 rule 15 deny icmp icmp-type echo
 rule 20 permit ip
```

从显示的结果可以看出，当前时间段 visit 处于非激活状态，此时进行测试会发现外部网络主机无法访问内网主机 192.168.1.2 上的 HTTP 服务。这是因为当前路由器的系统时间并没有处于时间段 visit 之内，此时的访问请求无法匹配第 1 条规则，而是匹配了规则 deny tcp 而被拒绝。

可以通过在用户视图下使用 clock datetime 修改当前的系统时间，使其处于时间段 visit 之内。具体如下：

```
<RTA>clock datetime 10:00 2011/11/5
```

修改完成后，时间段 visit 将处于激活状态，此时进行测试会发现外部网络主机可以访问内网主机 192.168.1.2 上的 HTTP 服务，说明定时 ACL 配置正确。

需要注意的是，在配置了定时 ACL 后往往需要对系统时间进行修改以测试定时 ACL 的执行效果。但是在测试完成后，一定要将系统时间修改回准确的时间，以避免在网络运行的过程中出现访问控制的错误。

2.6　H3C 基于应用层的包过滤技术

传统的以 ACL 为核心的包过滤属于静态包过滤技术，它只能根据数据报文中的特定信息如协议类型、IP 地址、端口号以及一些标志位来过滤流量，并不能检测和记录通信过程和连接状态，因此在实际网络应用中会存在以下 4 个问题。

(1) 静态包过滤技术虽然可以根据端口号来识别特定的应用层服务，但是它无法理解特定服务的上下文会话，因此对于多通道的应用层协议，会因为无法预知后续动态协商的数据通道信息而无法为其制定完善的安全过滤策略。例如，对于 FTP 协议，如果内部网络的 FTP 客户端使用主动模式访问外部网络的 FTP 服务器，由于无法提前预知 FTP 客户端进行监听的数据端口号，因而无法为其定义相应的 ACL 规则，导致无法建立 FTP 的数据连接。

(2) 无法检测来自于应用层的攻击行为。由于静态包过滤技术并不对报文的应用层内容进行解析和检测，因此无法对一些来自于应用层的威胁进行防范。例如，无法防范来自不可信网站的 Java Applet 或 Active X 插件对内部主机的破坏。

(3) 无法检测恶意的 TCP 响应报文和基于 UDP 报文的攻击。虽然静态包过滤技术可以使用 established 关键字来防范外部网络的主动 TCP 请求，但是无法对伪装成 TCP 响应报文的攻击流量进行防范；由于 UDP 协议是一种无连接协议，静态包过滤技术同样

无法对其攻击流量进行防范。

(4) 缺乏有效的日志功能。静态包过滤技术仅对静态的报文特征信息进行过滤和输出日志记录,不能对整个应用连接输出日志记录,因此无法实现对于应用连接的跟踪。

为解决以ACL为核心的静态包过滤技术存在的问题和不足,引入基于应用层的包过滤技术(Application Specific Packet Filter,ASPF)。与静态包过滤技术相比ASPF具有以下优点。

(1) 支持传输层协议检测(通用TCP/UDP检测)和ICMP、RAWIP协议检测。

(2) 支持对应用层协议的解析和连接状态的检测,这样每一个应用连接的状态信息都将被ASPF维护并用于动态地决定数据包是否被允许通过防火墙或丢弃。

(3) 支持应用协议端口映射(Port to Application Map,PAM),允许用户自定义应用层协议使用非通用端口。

(4) 支持Java阻断和ActiveX阻断功能,分别用于实现对来自于不信任站点的Java Applet和ActiveX的过滤。

(5) 支持ICMP差错报文检测,可以根据ICMP差错报文中携带的连接信息,决定是否丢弃该ICMP报文。

(6) 支持TCP连接首包检测,通过检测TCP连接的首报文是否为SYN报文,决定是否丢弃该报文。

(7) 提供了增强的会话日志和调试跟踪功能,可以对所有的连接进行记录,可以针对不同的应用协议实现对连接状态的跟踪与调试。

可见,ASPF技术不仅能弥补静态包过滤技术在应用中的缺陷,提供针对应用层的报文过滤,还具有多种增强的安全特性,是一种智能的高级过滤技术。

2.6.1 ASPF的工作原理

ASPF工作的基本原理是监听并记录应用协议的交互过程,并按照应用协议的特定需求动态创建访问控制列表,以达到精确控制报文转发的目的。在路由器上配置了ASPF之后,基于ASPF的包过滤将会对ASPF策略中定义的需要进行审查的协议产生的每一个会话进行检测和跟踪,并创建一个连接状态表和一个临时访问控制列表(Temporary Access Control List,TACL),以允许该会话的返回流量通过。

1. 传输层协议检测

传输层协议检测是指对数据报文的传输层及以下的信息,例如对报文的源IP地址、目的IP地址、端口号、传输层状态等进行的检测,包括TCP协议检测和UDP协议检测。

(1) TCP协议检测

TCP协议检测是指ASPF检测TCP连接发起和结束的状态转换过程,包括连接发起的3次握手状态和连接关闭的4次握手状态,然后根据这些状态来创建、更新和删除设备上的连接状态表。TCP检测是其他基于TCP的应用协议检测的基础。

TCP协议检测的具体过程:当ASPF检测到TCP连接发起方的第一个SYN报文时,开始建立该连接的一个连接状态表,用于记录并维护此连接的状态,并创建一个临时

访问控制列表来允许后续该连接的相关报文能够通过防火墙，而其他的非相关报文则被阻断和丢弃。具体如图 2-7 所示。

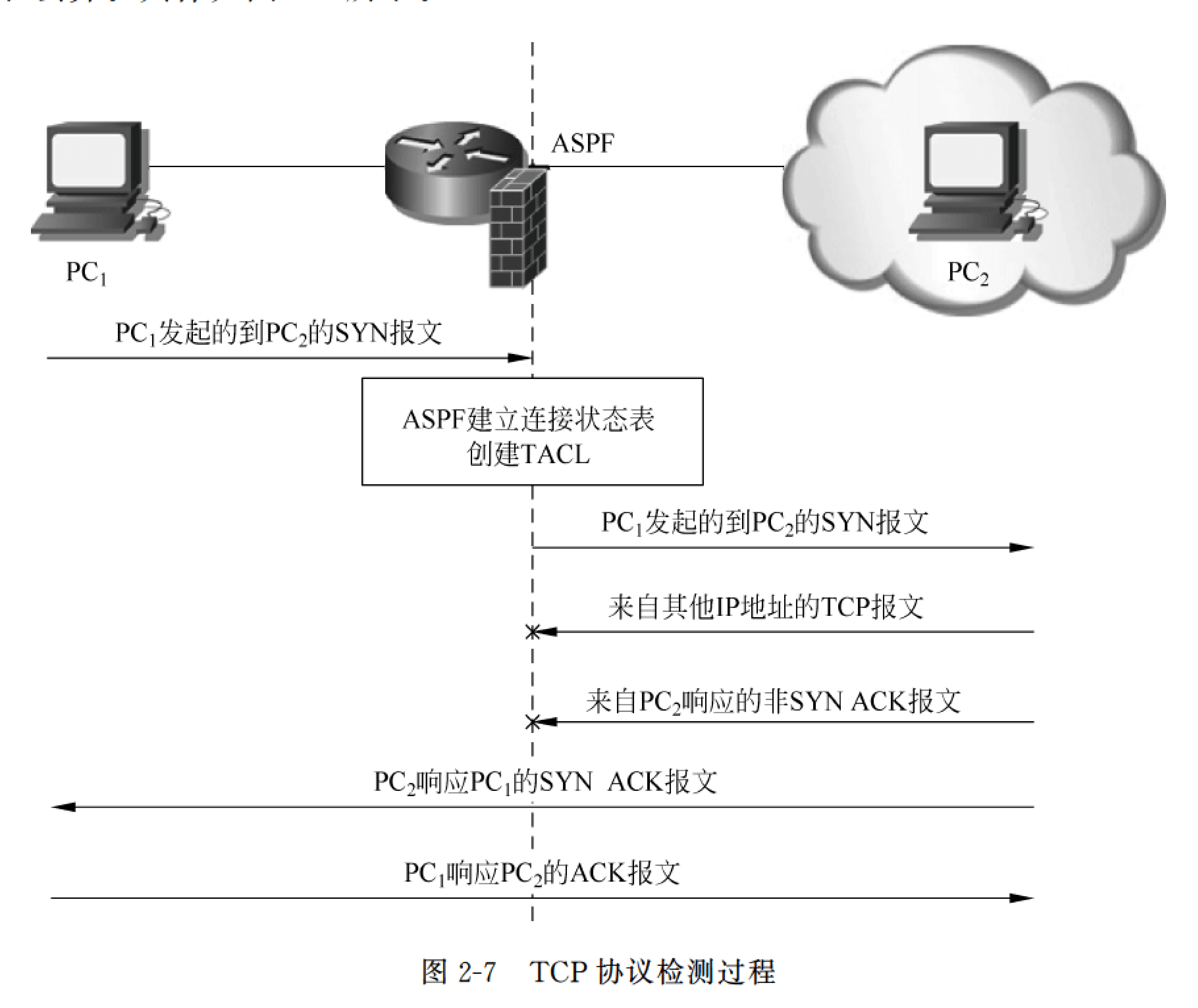


图 2-7 TCP 协议检测过程

（2）UDP 协议检测

UDP 协议没有连接状态的概念，ASPF 的 UDP 检测是指针对 UDP 连接的 IP 地址和端口进行的检测。UDP 检测是其他基于 UDP 应用协议检测的基础。

UDP 检测的具体过程：当 ASPF 检测到 UDP 连接发起方的第一个数据报文时，ASPF 开始维护此连接的信息。当 ASPF 收到接收方回送的 UDP 数据报时，此连接才能建立，其他与此连接无关的报文则被阻断和丢弃。

2. 应用层协议检测

应用层协议检测是 ASPF 通过创建连接状态表来跟踪和维护特定的应用层协议产生的连接某一时刻所处的状态信息，并依据该连接的当前状态来匹配后续的报文。ASPF 并不能对所有的应用层协议提供检测支持，目前 ASPF 可以支持的应用层协议包括 HTTP、FTP、SMTP、RTSP（Real Time Streaming Protocol，实时流协议）和 H. 323 音视频协议等。

对于单通道应用层协议，例如 HTTP、SMTP 等，ASPF 的检测过程相对比较简单，在发起连接时建立连接状态表和 TACL，连接删除时将连接状态表和 TACL 删除即可。而对于多通道应用层协议的检测就相对复杂一些。在对多通道应用层协议进行检测时，ASPF 可以对控制连接上传递的协商建立数据通道的报文进行解析和记录，从中获得建立数据通道的端口信息，从而创建相应的 TACL 来允许数据通道的建立和数据的传输。

ASPF 对典型的多通道应用层协议——FTP 协议的检测过程如图 2-8 所示。

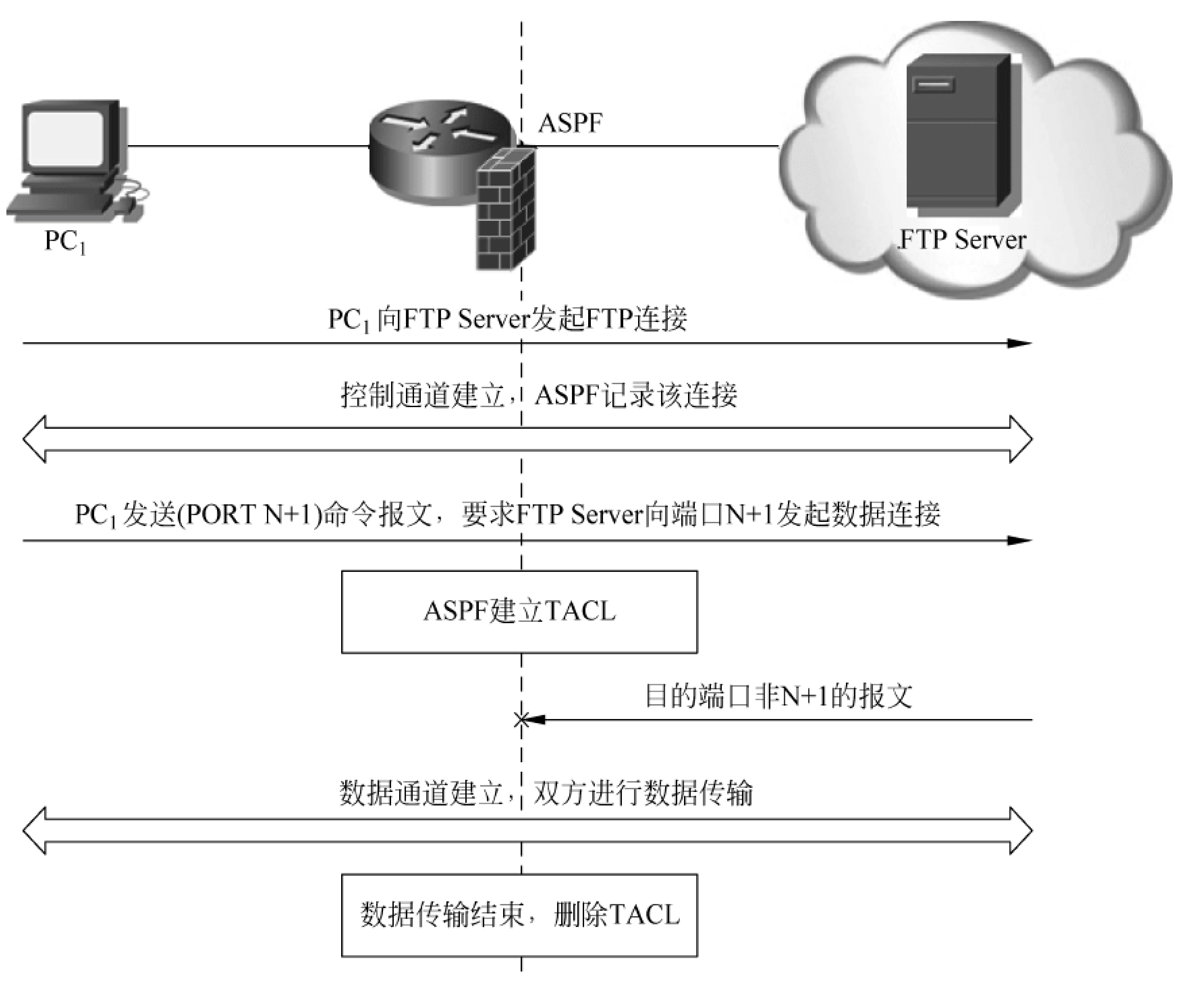


图 2-8　FTP 协议检测过程

在图 2-8 中，FTP 使用主动模式进行连接。ASPF 可以对 FTP 客户端发送给 FTP 服务器的建立数据连接命令“PORT N+1”进行解析，从中获得 FTP 客户端监听的数据端口为“N+1”，并为之建立 TACL，从而允许数据通道的建立和数据的传输。

2.6.2　ASPF 的配置和验证

ASPF 的配置相对比较简单，同样需要启动防火墙功能，在此不再赘述。具体配置涉及的命令如下。

(1) 创建一个 ASPF 策略。*aspf-policy-number* 的取值范围为 1～99。

[H3C] aspf-policy *aspf-policy-number*

(2) 在 ASPF 策略视图下配置基于传输层协议和应用层协议的审查规则。

[H3C-aspf-policy-1]detect *protocol* [java-blocking *acl-number*] [aging-time *seconds*]

其中各个参数的解释如下。

protocol：定义审查的协议类型，可以选取 HTTP、FTP、SMTP、RTSP、H323、TCP 和 UDP 协议。

java-blocking *acl-number*：配置 Java 阻断功能，其中，*acl-number* 是标识可信任的与不可信任的主机或网段的基本 ACL 编号。当 ASPF 配置了支持 Java 阻断功能的 HTTP 协议检测时，受保护网络内的用户如果试图通过 Web 页面访问不可信站点，则 Web 页面

中为获取包含 Java Applet 程序而发送的请求指令将会被 ASPF 阻断。

aging-time *seconds*：设置 TACL 的超时时间。默认情况下应用层协议和 TCP 协议的超时时间均为 3600s；UDP 协议的超时时间为 30s。

（3）将 ASPF 应用到特定接口的特定方向上。

```
[H3C-Ethernet0/0]firewall aspf aspf-policy-number { inbound | outbound }
```

虽然 ASPF 可以应用在 inbound 和 outbound 两个方向上，但实际上 ASPF 一般都会应用在出口路由器与外部网络连接接口的 outbound 方向上，用于对内部网络访问外部网络的流量进行审查。而且要求在该接口的 inbound 方向上应用一个 ACL，用来承载 ASPF 产生的 TACL。ASPF 产生的 TACL 规则总是放置在其承载 ACL 的静态规则之前。实际上，如果在出口路由器与外部网络连接接口的 inbound 方向上没有应用 ACL，则外部网络可以随意访问内部网络，也就没有对内部网络访问外部网络的流量进行审查的必要。

在此依然使用图 2-5 所示的网络，要求允许内部网络的主机访问外部网络的 FTP 和 HTTP 服务，但是禁止其他的访问。具体的配置命令如下：

```
[RTA]firewall enable
[RTA]aspf-policy 1
[RTA-aspf-policy-1]detect ftp
[RTA-aspf-policy-1]detect http
[RTA-aspf-policy-1]quit
[RTA]acl number 3000
[RTA-acl-adv-3000]rule deny ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall aspf 1 outbound
[RTA-Ethernet0/1]firewall packet-filter 3000 inbound
```

这里需要注意，虽然 FTP 协议和 HTTP 协议在传输层同样由 TCP 协议承载，但是并不能使用 detect tcp 命令来代替 detect ftp 和 detect http 命令。因为对于像 FTP 这样的多通道应用层协议，在不配置应用层检测而直接配置 TCP 检测的情况下，会导致数据连接无法建立(实际上在这个例子中如果 FTP 使用主动模式连接会导致数据连接无法建立，而如果 FTP 使用被动模式则没有影响)。

配置完成后，在路由器 RTA 上使用命令 display aspf all 查看 ASPF 的策略信息如下：

```
[RTA]display aspf all
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                  disable
    SYN timeout:          30s
    FIN timeout:          5s
    TCP timeout:          3600s
    UDP timeout:          30s
```

```
    Detect Protocols:
      HTTP timeout 3600s
      FTP    timeout 3600s

[Interface Configuration]
   Interface                         InboundPolicy    OutboundPolicy
-------------------------------------------------------------------------
   Ethernet0/1                         none               1
```

从显示的结果可以看出,在路由器 RTA 上配置了一个 ASPF 策略,策略编号为 1,该策略对 HTTP 协议和 FTP 协议进行审查,HTTP 协议和 FTP 协议的超时时间均为 3600s。策略被应用在了接口 Ethernet 0/1 的 outbound 方向上。

此时,外部网络主机将无法访问内部网络的任何服务,但在内网主机 PC_1 或 PC_2 上连接外部网络中主机 192.168.4.2 上的 FTP 服务和 HTTP 服务,可以连接。在路由器 RTA 上使用命令 display aspf session 查看 ASPF 的会话信息如下:

```
[RTA]display aspf session

There are 3 ASPF sessions:
[Established Sessions]
Session Initiator              Responder            Application     Status
------------------------------------------------------------------------------------------
7F55090 192.168.1.2:3859       192.168.4.2:21       FTP             FTP_CONXN_UP

7F571B0 192.168.1.2:3985       192.168.4.2:80       HTTP            TCP_READY

[Terminating Sessions]
Session Initiator              Responder            Application     Status
------------------------------------------------------------------------------------------
7F573F0 192.168.1.2:3988       192.168.4.2:3996     FTP-data        TCP_CLOSING
```

从显示的结果可以看出,ASPF 在内部网络主机 192.168.1.2 和外部网络主机 192.168.4.2 之间建立了基于 FTP 协议和 HTTP 协议的会话。

在用户视图下使用命令 reset aspf session 可以清除 ASPF 的会话信息。

2.7 Cisco 反射 ACL 技术

2.7.1 反射 ACL 简介

扩展 ACL 是无状态的 ACL,配置了扩展 ACL 的网络设备只是根据数据报文中的标志、类型等过滤流量,并不记录通信过程,因此不能用于防范恶意用户利用各类响应报文或无状态报文发动的攻击。举例如下。

(1) 使用扩展 ACL 可以拒绝外网对内网的 ICMP echo 报文,但考虑到要允许内网对外网的 ping 能够成功,所以需要允许外网送到内网的 ICMP echo-reply 流量。由于扩展 ACL 只是检查 ICMP 报文类型,所以不能用于防范恶意用户使用 smurf 发送大量 ICMP echo-reply 到内网的攻击。

(2) 扩展 ACL 可以通过 established 关键字,只允许外网的响应报文进入内网,但是不能用于防范恶意用户发送大量 TCP 响应报文攻击内网。

(3) UDP 协议通信时没有建立连接的过程,不能使用类似 established 关键字的扩展 ACL 来限制外网送到内网的 UDP 流量。恶意用户可以利用这一安全漏洞,使用像 Fraggle 这样的工具,向内网发送大量 UDP 报文进行 DoS 攻击。

反射 ACL 技术是一种解决以上安全问题的简易手段。

反射 ACL 技术的基本原理:来自有效源主机的流量会触发(反射)一个允许该连接返回流量的临时 ACL,允许该连接的返回流量进入网络。

一旦反射 ACL 被产生,则会自动启动一个定时器,超时后反射 ACL 失效。

2.7.2　反射 ACL 配置方法

反射 ACL 的配置步骤如表 2-5 所示,主要配置工作包括在路由器到外网方向上定义带有 reflect 关键字的 ACL 过滤条目,使之能产生允许返回流量的 ACL,然后在路由器到内网方向上定义带有 evaluate 命令的 ACL 过滤条目,在入站方向上指定反射 ACL 过滤条目的正确位置。

表 2-5　反射 ACL 配置步骤

序号	操　　作	相 关 命 令	必要性
步骤 1	定义从内网到外网的 ACL,并在需要允许返回流量的命令后增加"reflect"	ip access-list permit ...reflect	是
步骤 2	定义从外网到内网的 ACL,引用反射 ACL	ip access-list evaluate ...	是
步骤 3	在网络设备接口上应用各方向上定义的 ACL	ip access-group	是
步骤 4	检查反射 ACL 配置	show access-list show ip interface	可选 可选

如果要允许某个 permit 命令定义的流量能够产生反射 ACL,则可以输入:

permit {tcp ...|udp ...} reflect *reflect-acl-name* timeout *second*

该命令将为匹配的流量创建一个指定名字的反射 ACL 过滤条目,以允许相应返回的流量。

参数 *second* 用于指定多长时间后该反射 ACL 失效,单位为秒(s),范围为 1~2147483,默认值为 300。

配置外网到内网方向上的 ACL 中,引用所定义反射 ACL 条目的操作为,在该 ACL 配置模式下输入:

evaluate *reflect-acl-name*

需要注意的是,Cisco 网络设备不会在反射 ACL 过滤条目末尾隐含增加拒绝所有流量的语句。

为限制外网主动向内网发起TCP连接以及向内网主动发送UDP报文的配置如下所示。

```
Router1(config)#ip access-list extended in2out                                    ①
Router1(config-ext-nacl)#permit tcp any any reflect racl-tcp                      ②
Router1(config-ext-nacl)#permit udp any any reflect racl-udp timeout 30           ③
Router1(config-ext-nacl)#permit ip any any                                        ④
Router1(config-if)#exit
Router1(config)#ip access-list extended out2in                                    ⑤
Router1(config-ext-nacl)#evaluate racl-tcp                                        ⑥
Router1(config-ext-nacl)#evaluate racl-udp                                        ⑦
Router1(config-ext-nacl)#deny tcp any any                                         ⑧
Router1(config-ext-nacl)#deny udp any any                                         ⑨
Router1(config-ext-nacl)#permit ip any any                                        ⑩
Router1(config-if)#exit
Router1(config)#interface fa0/1
Router1(config-if)#ip access-group out2in in                                      ⑪
Router1(config-if)#ip access-group in2out out                                     ⑫
Router1(config-if)#end
Router1#show ip access-lists
Extended IP access list in2out
    10 permit tcp any any reflect racl-tcp (123 matches)
    20 permit ip any any (19 matches)
Extended IP access list out2in
    20 evaluate racl-tcp
    30 deny tcp any any (39 matches)
    40 permit ip any any (62 matches)
Reflexive IP access list racl-tcp
     permit tcp host 200.100.10.2 eq telnet host 10.10.10.2 eq 11002 (45 matches)  ⑬
(time left 296)
```

以上配置说明如下。

① 定义一个名为"in2out"的扩展ACL,该ACL将用于从内网到外网的流量过滤。根据安全需求,不禁止任何从内网到外网的IP流量,但需要检查内网到外网的TCP、UDP流量,以触发生成反射ACL。

② 该过滤条目用于产生反射ACL以允许从外网到内网的TCP响应流量。

③ 该过滤条目用于产生反射ACL以允许从外网到内网的UDP响应流量,为防范恶意用户利用定时器默认300s的间隔发动UDP攻击,因此将定时器设置为30s。

④ 该过滤条目用于允许除TCP流量外其他从内网到外网的IP流量。

⑤ 定义一个名为"out2in"的扩展ACL,该ACL将用于从外网到内网的流量过滤。

⑥ 在扩展ACL"out2in"中引用允许TCP响应流量的反射ACL条目。

⑦ 在扩展ACL"out2in"中引用允许UDP返回流量的反射ACL条目。

⑧ 拒绝其他TCP流量。

⑨ 拒绝其他UDP流量。

⑩ 允许其他IP流量。

⑪ 在路由器连接外网的接口fa0/1入站方向上应用所定义的"out2in"ACL。

⑫ 在路由器连接外网的接口 fa0/1 出站方向上应用所定义的“in2out”ACL。

⑬ 在内网 10.10.10.2 主机上使用 Telnet 远程登录 200.100.10.2 所触发的反射 ACL。

2.8 Cisco 基于上下文的访问控制技术

2.8.1 CBAC 简介

基于上下文的访问控制(Context-based Access Control,CBAC)是 Cisco IOS 防火墙安全特性集中的一项特性,它比反射 ACL 具有更多的安全功能。

CBAC 提供以下 4 项功能。

(1) 可以对应用层流量进行状态审查,如发起连接的速率、TCP 序号范围等。

(2) 能够根据应用层信息过滤流量。

(3) 通过进行流量审查等,可以检测某些类型的 DoS 攻击。

(4) 能实时生成警告、审查跟踪信息。

CBAC 工作过程与反射 ACL 很相似。如图 2-9 所示,如果在内网到外网的接口上配置 CBAC 审查流出内网的流量,则当流量通过审查时,将触发建立一个临时的从外网到内网入口 ACL 条目,允许对应该连接外网到内网的返回流量。同时,CBAC 利用一个状态表,记录所监控(审查)连接的状态信息。在对流量进行 CBAC 审查时,网络设备会检查状态表中是否已经存在该连接。如果不存在,则会在状态表中添加该连接相应的条目;如果连接已经存在,就将对应条目的空闲超时清零。

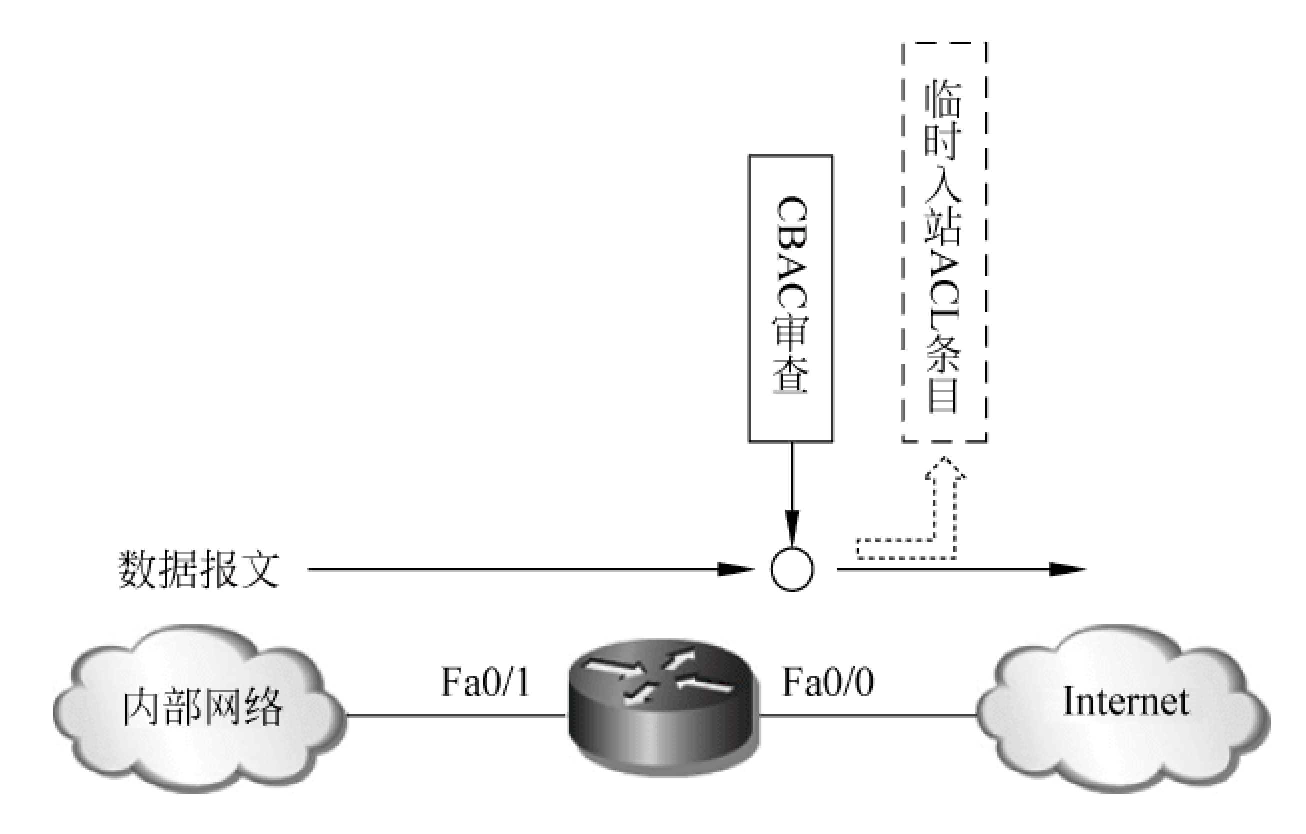


图 2-9 CBAC 审查与临时 ACL 条目

1. TCP 流量审查

CBAC 审查 TCP 流量时,检查 TCP 报文头中的控制位和 TCP 连接状态。

(1) 如果配置在第 1 个 SYN 报文之后的 30s 内应建立连接,而在此时间内连接没有建立,则 CBAC 会从状态表和 ACL 中删除由第 1 个 SYN 报文触发创建的条目。

(2) 如果检查到 1 个 TCP 连接空闲超过 1h,则 Cisco IOS 会从状态表和 ACL 中删除对应的条目。

(3) 如果检查到 TCP 报文中有 FIN 标志,则 5s 之后还没有收到后续响应报文,

Cisco IOS 会从状态表和 ACL 中删除对应的条目。

(4) 如果收到的 TCP 报文头中序号与所期望范围不符,则 CBAC 会丢弃这些数据报文,并会认为有欺骗或 DoS 发生。

2. UDP 流量审查

CBAC 审查 UDP 流量时,与反射 ACL 处理相同,都是通过估计 UDP 会话的生命期来进行相应处理。如果配置一个 UDP 会话空闲时间应为 30s,则如果 30s 内该会话上没有 UDP 流量通过,则 Cisco IOS 会从状态表和 ACL 中删除对应的条目。

另外对于 DNS 的 UDP 流量,如果配置 CBAC 审查发出的 DNS 请求,并且 5s 内应能从 DNS 服务器处获得 DNS 答复,则当 5s 内没有收到答复的情况下,Cisco IOS 会从状态表和 ACL 中删除对应的 DNS 条目;而一旦在 5s 内收到了 DNS 服务器的答复,则 Cisco IOS 也会立即从状态表和 ACL 中删除对应的 DNS 条目。

3. ICMP 流量审查

CBAC 对 ICMP 流量的审查只在 12.2(11)版本以后的 Cisco IOS 中才支持。目前 CBAC 只能审查几种常见的 ICMP 消息,如 echo、echo-reply、host-unreachable、timestamp-request、timestamp-reply 等。CBAC 审查 ICMP 流量时,如果 10s 内没有相应的 ICMP 回应信息返回,则从状态表和 ACL 中删除对应的连接条目;如果 10s 内收到相应的 ICMP 回应,则检查这些信息,只有被支持的 ICMP 信息能够通过,其他类型的 ICMP 信息被丢弃。

4. 附加连接处理与 NAT 流量处理

(1) 附加连接处理

以 FTP 连接为例,FTP 客户端在使用端口 1024 与 FTP 服务器 21 端口建立起 FTP 连接后,如果使用被动模式下载文件,则 FTP 客户端会使用一个新的端口与 FTP 服务器建立连接。反射 ACL 由于无法为该附加连接建立相应的动态 ACL 条目,因此使用反射 ACL 的网络,就只能使用主动 FTP 模式的 FTP 服务。CBAC 可以解决这一问题,CBAC 会审查 FTP 客户端与 FTP 服务器间应用层流量,然后根据 FTP 流量中的信息分别在状态表、ACL 中为附加连接建立相应的条目。

(2) NAT 流量处理

在配置了 NAT 和 CBAC 的路由器上,对于从外网入站的返回流量,路由器先处理状态表,然后是 ACL,最后才是 NAT。为了保证状态表中有正确的返回连接条目,同时入站 ACL 中有正确的返回连接 ACL 条目,CBAC 会在流量从内网到外网时,使用审查功将内网主机的全局地址动态连接条目加入状态表和 ACL。

5. CBAC 对 DoS 攻击的检测

CBAC 可以检测并在一定程度上抵御 DoS 攻击。可以配置 TCP 连接的超时值、TCP 连接数量的阈值,使得 CBAC 审查 TCP 流量时,可以检测到网络中是否存在大量来自单一源地址的 TCP SYN 报文,是否存在指定时间段仍未完成的 TCP 连接。以下为 3 种常用保护内网主机的阈值。

(1) TCP 半连接或未完成的 UDP 会话数。

（2）一定时间内 TCP 半连接或未完成会话总数。

（3）每个主机 TCP 半连接总数。

2.8.2　CBAC 配置方法

在 Cisco IOS 中配置 CBAC 的基本步骤如表 2-6 所示。其中，第 1、2 步用于定义和接口上应用过滤流量的 ACL，CBAC 审查产生的动态 ACL 条目会加入到这些 ACL 中；第 3 步用于定义 CBAC 审查规则，该步定义 CBAC 审查哪些协议的流量；第 4 步指定各类协议的超时值，主要用于防范 DoS 攻击；当被审查的网络服务使用了非知名的服务端口来提供服务时，使用第 5 步操作定义端口映射，明确 CBAC 应审查哪些端口；第 6 步定义在哪些流量上应用 CBAC 审查规则；第 7 步对 CBAC 配置进行检查，确保 CBAC 配置正确。

表 2-6　CBAC 基本配置步骤

序号	操　作	相 关 命 令	是否必要
步骤 1	定义 ACL	access-list 或 ip access-list	是
步骤 2	在接口应用 ACL	ip access-group	是
步骤 3	定义审查规则	ip inspect	是
步骤 4	定义全局超时值，用于防范 DoS	ip inspect	可选
步骤 5	定义端口映射，用于审查使用非知名端口提供的服务	ip port-map	根据网络服务情况使用
步骤 6	在接口应用审查规则	ip inspect	是
步骤 7	检查 CBAC 配置	show ip inspect debug ip inspect	可选

1. 定义并应用 ACL

在配置 CBAC 时需要注意，只有在相应接口上已经配置应用了扩展 ACL 时，CBAC 才能将审查流量产生的动态 ACL 条目添加到该 ACL 中。

例如图 2-10 中，当为保护内部网络 10.0.0.0/24 的安全而在 Router1 配置 CBAC 时，需要首先保证在 Fa0/0 入站方向上配置有扩展 ACL，这样由 CBAC 审查产生的动态 ACL 才能添加到该扩展 ACL 中。注意，必须是扩展 ACL 才能使 CBAC 正常工作，因为 CBAC 产生的动态 ACL 条目包含有源地址、目的地址、协议类型等扩展 ACL 才有的信息。

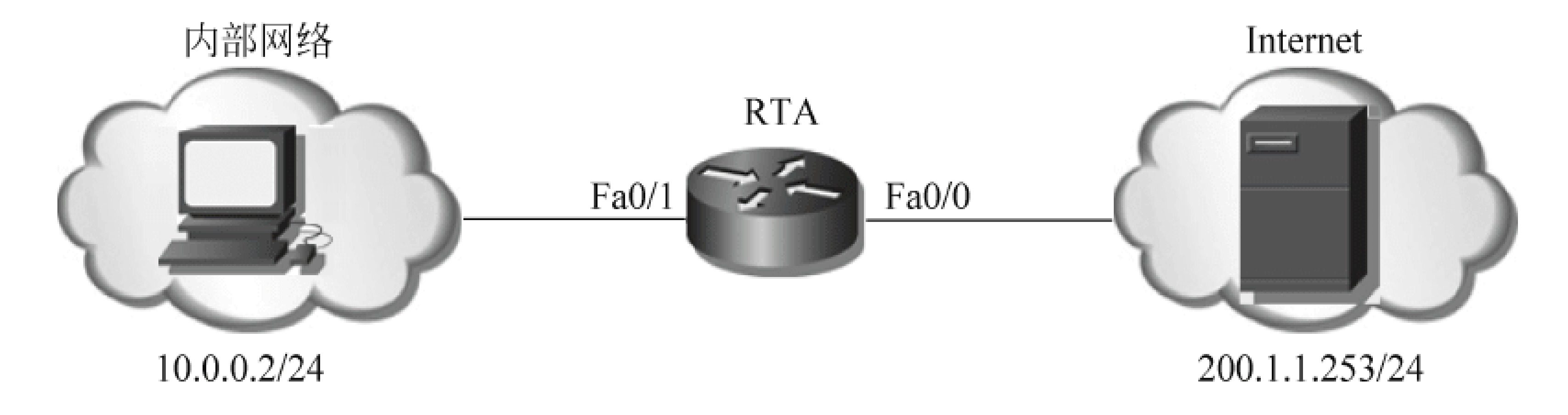


图 2-10　CBAC 配置示例 1

2. 定义及应用审查规则

（1）定义审查规则

在 Cisco IOS 中定义审查规则的操作为在全局配置模式下输入：

ip inspect name *inspection-name* {*protocol* |fragment maximum *fragment-number*} [alert {on|off}] [audit-trail {on|off}] [timeout *second*]

其中,*inspection-name* 参数为该组审查规则在网络设备上的唯一标识。可以通过定义使用同一个审查规则组名的多条审查规则而将多条审查规则绑定在一起。

protocol 参数定义该审查规则审查哪种协议的流量,该协议必须为 CBAC 支持的协议,如表 2-7 所示。

表 2-7 CBAC 支持的协议

协议名关键字	说　明
cuseeme	CUSeeMe 协议
ftp	文件传输协议
h323	H. 323 协议,例如 MS NetMeeting、Intel Video Phone
http	超文本传输协议
icmp	ICMP 协议
netshow	微软 NetShow 协议
rcmd	远程命令行协议,例如 r-exec、r-login、r-sh
realaudio	Real Audio 协议
rpc	远程过程调用协议
rtsp	Real Time Streaming Protocol
sip	SIP 协议
skinny	Skinny 客户端控制协议,思科专有协议
smtp	简单邮件传输协议
sqlnet	SQL Net Protocol
streamworks	StreamWorks Protocol
tcp	传输控制协议
tftp	TFTP 协议
udp	用户报文协议
vdolive	VDOLive Protocol

fragment 关键字和后面的最大值定义 CBAC 允许会话包含分片的最大数量。

alert 关键字和后面的 on、off 关键字用于定义是否打开警告。

audit-trail 关键字和后面的 on、off 关键字用于定义是否打开审查审计。

timeout 关键字和后面的 *second* 参数用于定义该类会话的超时时间。此处如果未定义超时时间,还可以使用在全局模式下配置的全局超时时间。

(2) 应用审查规则

在 Cisco IOS 中定义审查规则的操作为在接口配置模式下输入:

ip inspect name *inspection-name* {in|out}

其中,*inspection-name* 为前面所定义的审查规则组名。

关键字 in、out 用于指定对接口哪个方向的流量进行审查。

例如,要禁止从 Internet 向内部网络主动发起 TCP 连接,但允许内部网络向 Internet 主动发起 TCP 连接,则可以在 Router1 上进行如下配置。

```
Router1(config)# ip access-list extended eacl-out2in                    ①
Router1(config-ext-nacl)# deny tcp any 10.0.0.0 0.0.0.255               ②
Router1(config-ext-nacl)# permit ip any any                             ③
Router1(config-ext-nacl)# exit
Router1(config)# ip inspect name cbac tcp                               ④
Router1(config)# interface fa0/1
Router1(config-if)# ip inspect cbac in                                  ⑤
Router1(config)# interface fa0/0
Router1(config-if)# ip access-group eacl-out2in in                      ⑥
```

以上配置说明如下。

① 创建名为"eacl-out2in"的扩展 ACL，该扩展 ACL 将被应用到 Router1 连接 Internet 的接口入站方向上，用于过滤来自 Internet 的主动 TCP 连接。

② 拒绝所有对内部网络 10.0.0.0/24 的 TCP 流量。由于 CBAC 审查会自动在该 ACL 最前面动态增加 Internet 返回内部网络的 TCP 流量，所以这里使用该命令拒绝所有其他的 TCP 流量。

③ 允许所有 IP 流量，以保证其他流量不受影响。

④ 定义一个组名为"cbac"的审查规则，该审查规则对 TCP 流量进行检查。

⑤ 在 Router1 连接内部网络的入站方向上应用已定义的审查规则"cbac"，审查所有内部网络经由 Router1 接口 fa0/1 进入路由器的 TCP 流量。

⑥ 在 Router1 连接 Internet 的入站方向上应用已定义的扩展 ACL"eacl-out2in"，过滤所有来自 Internet 的流量。

3. 定义全局超时值及半连接最大值

如前所述，可以定义各类协议的超时值来防御 DoS 攻击。一些常用的超时值定义命令如表 2-8 所示。

表 2-8　常用的超时值定义命令

ip inspect tcp synwait-time	TCP 会话建立时间①
ip inspect tcp finwait-time	TCP 会话拆除时间②
ip inspect tcp idle-time	TCP 会话空闲时间③
ip inspect udp idle-time	UDP 会话空闲时间④
ip inspect dns-timeout	DNS 查询时间⑤
ip inspect tcp max-incomplete host	单机半连接最大值⑥

注：① 定义 TCP 连接建立，即 3 次握手的最长时间。如果状态表中已有条目超过此时间定义仍未完成 TCP 连接建立过程，则 CBAC 会自动删除状态表中该条目以及 ACL 中动态添加的相应 ACL 条目。该超时值默认为 30s。

② 定义开始一个 TCP 会话的拆除过程多长时间后从状态表中删除该 TCP 连接条目。其默认值为 5s。

③ 定义状态表中一个 TCP 会话多长时间内没有相应的 TCP 流量经过，则 CBAC 会将其状态表条目和 ACL 中相应条目删除。其默认值为 3600s。

④ 定义状态表中一个 UDP 会话多长时间内没有相应的 UDP 流量经过，则 CBAC 会将其状态表条目和 ACL 中相应条目删除。其默认值为 30s。

⑤ 定义状态表中一个 DNS 请求多长时间还未收到答复后，CBAC 会将其状态表条目和 ACL 中相应条目删除。其默认值为 5s。

⑥ 定义每台主机的最大半连接会话数，范围为 1～4294967295。

4. 定义端口映射

CBAC审查各类网络应用协议时,默认按照此类网络应用协议的知名端口对其流量进行审查。当实际网络中的网络服务使用了非知名端口提供网络服务时,为保证CBAC工作正常,需要配置端口映射,以使得CBAC能够正确审查网络应用协议。

在Cisco IOS中定义端口映射的操作为在全局配置模式下输入:

ip port-map *application_name* port *port-number* [*acl-number*|*acl-name*]

其中,*application_name* 参数用于指定哪类网络服务使用了非知名端口。

port-number 参数用于定义该网络服务使用了什么端口。

可选参数 *acl-number*|*acl-name* 用于指定哪些网络中的主机在提供该类网络服务时使用了所定义的非知名端口。

配置完端口映射后,可以在特权模式下使用show ip port-map命令来查看端口映射配置情况。该命令语法如下:

show ip port-map [{*application_name*| port *port-number*]

该命令不带任何参数,则显示各类网络服务在Cisco IOS中默认对应的端口。

该命令带网络服务名参数,则显示指定网络服务的系统默认和用户使用端口映射自定义的端口。

该命令带port关键字和 *port-number* 参数,则显示系统中指定端口号对应的网络服务。

show ip port-map命令输出结果如下:

```
Router1(config)#ip port-map http port 80
Router1(config)#exit
Router1#show ip port-map http
Default mapping: http          port 8080          user defined
Default mapping: http          port 80            system defined
Default mapping: http          port 8090          user defined
Router1#  show   ip   port-map port 80
Default mapping: http          port 80            system defined
Router1#  show   ip   port-map
Default mapping: dns           port 53            system defined
...
Default mapping: http          port 80            system defined
```

5. 检查CBAC配置

在Cisco IOS中可以使用3种方法检查CBAC的配置是否符合要求,即show命令、debug命令、警告和审计。下面介绍show和debug命令。

(1) show 命令

在Cisco IOS中可以在特权模式下输入以下命令来查看CBAC审查执行情况。

show ip inspect {sessions|stat}

其中，使用 sessions 参数，将显示当前状态表中的会话条目。

使用 stat 参数，将显示到目前为止 CBAC 状态表会话条目的统计信息。

show ip inspect 命令的输出结果如下：

```
Router1#show ip inspect sessions
Established Sessions
Session 640008CC (10.0.0.254:0)=>(0.0.0.0:0) icmp SIS_OPEN                ①
Router1# show  ip  inspect  stat
Interfaces configured for inspection 1                                    ②
Session creations since subsystem startup or last reset 14                ③
Current session counts (estab/half-open/terminating) [0:0:0]              ④
Maxever session counts (estab/half-open/terminating) [0:1:0]              ⑤
Last session created 00:00:34
Last statistic reset never
Last session creation rate 1
Last half-open session total 0
```

输出结果说明如下：

① 当前状态表中有 1 条会话条目，该条目为主机 10.0.0.254 发出 ICMP 请求触发的条目。

② 截至命令执行时刻，已在 1 个接口上配置了 CBAC 审查。

③ 自从上次系统 CBAC 启动或重新设置开始到该命令执行时刻，状态表中共记录过 14 条会话。

④ 当前已建立、半连接、终止的会话条目数。

⑤ 已建立、半连接、终止的最大会话条目数。

(2) debug 命令

在 Cisco IOS 中可以在特权模式下输入以下命令来跟踪 CBAC 审查执行情况。

```
debug ip inspect protocol
```

参数"协议名"用于定义只显示被审查的 ICMP 流量。

该命令输出结果如下：

```
Router1#debug ip inspect icmp                                             ①
INSPECT ICMP Inspection debugging is on
Router1#
*Mar  1 05:50:11.306: CBAC ICMP: sis 640008CC pak 63C1BCCC SIS_CLOSED ICMP packet
(10.0.0.254:0) => (0.0.0.0:0) datalen 72                                  ②
*Mar  1 05:50:11.446: CBAC * ICMP: sis 640008CC pak 63E66810 SIS_OPENING ICMP
packet (10.0.0.254:0) <= (0.0.0.0:0) datalen 72                           ③
```

输出结果说明如下：

① 打开 ICMP 协议的 CBAC 审查跟踪。

② 在 10.0.0.254 上执行 ping 命令后 CBAC 的审查信息。

③ 收到返回给 10.0.0.254 的 ICMP 响应后 CBAC 的审查信息。

2.9 模拟公司分支机构网络边界安全ACL配置示例

模拟公司分支机构A-1网络拓扑结构如图2-11所示。

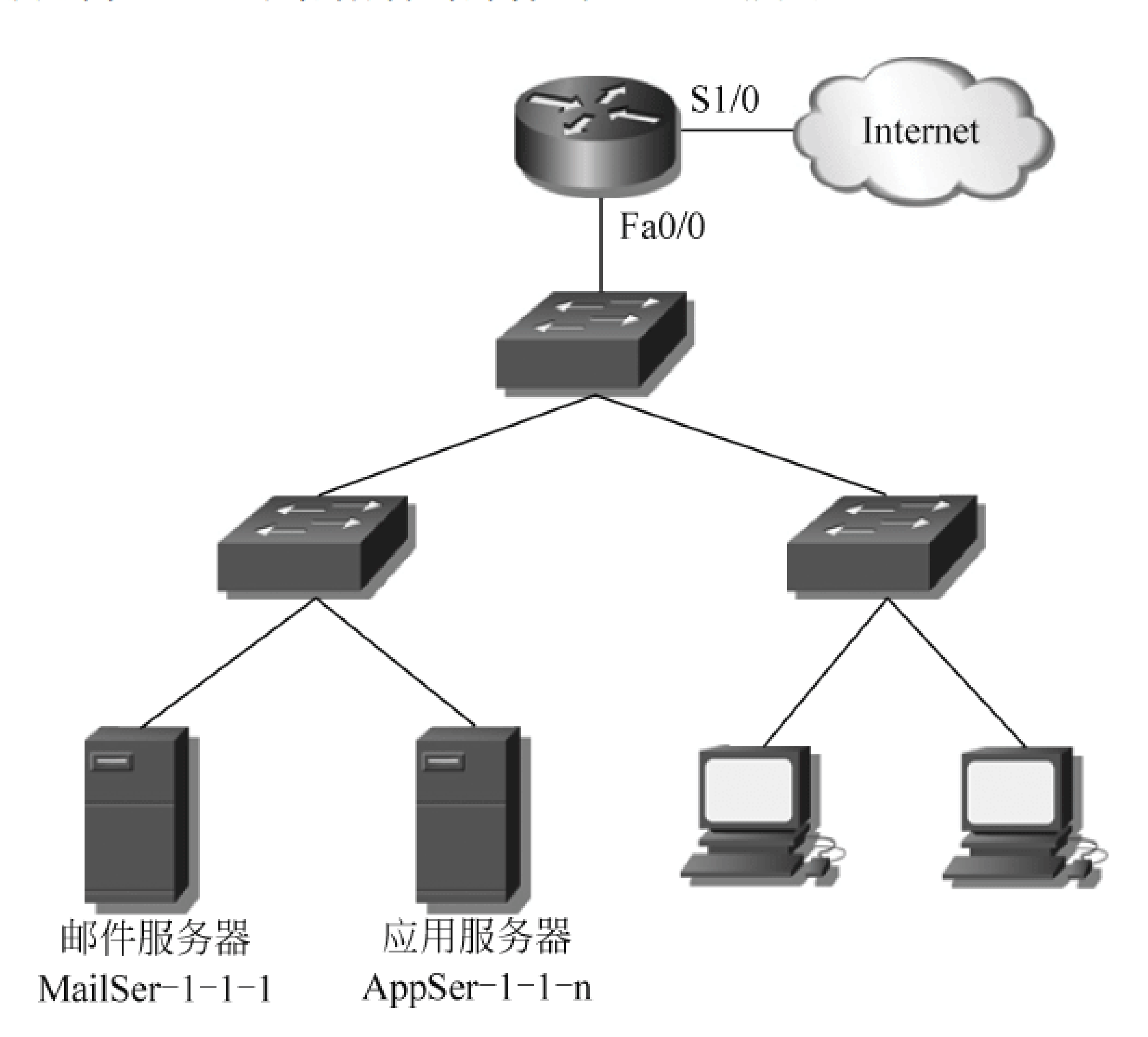


图2-11 分支机构A-1网络拓扑示意图

总公司及分支机构IP地址分配情况如表2-9所示。分支机构网络内IP地址分配情况如表2-10所示。其中各分支机构最后16个IP地址,分别作为网络设备管理地址和网络服务器IP地址。

表2-9 模拟公司IP地址分配

机 构	IP网络	可用IP地址数量
总公司	200.100.8.0/22	1022
分公司1	200.100.12.0/24	254
分公司2	200.100.13.0/24	254
分支A-1	200.100.14.0/25	126
分支A-2	200.100.14.128/26	62
分支A-3	200.100.14.192/26	62
分支B-1	200.100.15.0/26	62
分支B-2	200.100.15.64/26	62
分支C-1	200.100.15.128/27	30
分支C-2	200.100.15.160/27	30
串行链路1	200.100.15.192/30	2
串行链路2	200.100.15.196/30	2
串行链路3	200.100.15.200/30	2
串行链路4	200.100.15.204/30	2
串行链路5	200.100.15.208/30	2

续表

机　　构	IP 网络	可用 IP 地址数量
串行链路 6	200.100.15.212/30	2
串行链路 7	200.100.15.216/30	2
串行链路 8	200.100.15.220/30	2
串行链路 9	200.100.15.224/30	2

表 2-10　分支机构网络内 IP 地址分配

设　　备	IP 地址
分支 A-1 邮件服务器地址	200.100.14.117/29
分支 A-1 应用服务器地址	200.100.14.113～200.100.14.116/29
分支 A-1 网络设备管理地址	200.100.14.121～200.100.14.126/29
分支 C-2 邮件服务器地址	200.100.15.181/29
分支 C-2 应用服务器地址	200.100.15.177～200.100.15.180/29
分支 C-2 网络设备管理地址	200.100.15.185～200.100.14.189/29

在此以 Cisco 为例，按照第 2.1 节给出的安全配置方案进行分析，需要在边界路由器上进行的配置任务如下。

(1) 在边界路由器连接外网接口的入站方向上配置扩展 ACL，包含如下规则。

① 拒绝 bogon 主机对分支机构网络的 IP 流量。

② 配置定时 ACL 条目，允许到应用服务器指定端口的流量。

③ 允许到邮件服务器的邮件通信流量。

④ 允许到内网网络设备的 SSH 流量。

⑤ 允许从 Internet 到内网网络设备和服务器的 ICMP 流量。

⑥ 拒绝所有来自 Internet 的 TCP、UDP、ICMP 流量。

⑦ 允许来自 Internet IP 流量。

(2) 在边界路由器连接外网接口的出站方向上配置 CBAC 条目 cbac，允许从 Internet 返回的 TCP、UDP、ICMP 流量。

(3) 在边界路由器连接分支网络的各子接口入站方向配置拒绝所有 TCP 和 UDP 1524 端口、27444 端口、27665 端口、16660 端口、65000 端口、31335 端口，IRC 服务的 TCP 6665～6669 端口和木马常用端口流量。

(4) 在边界路由器连接分支网络的各子接口入站方向配置 CBAC 审查 TCP、UDP、ICMP 流量，与接口 S1/0 入站方向上扩展 ACL 条目配合，拒绝所有 Internet 到分支机构网络内除服务器外其他主机的主动连接。

(5) 在分支网络所有网络设备 VTY 线路上配置标准 ACL，拒绝 bogon 地址主机但允许其他主机使用 SSH 远程登录管理网络设备。

具体的配置如下：

```
ip inspect name cbac tcp                                          ①
ip inspect name cbac udp timeout 30
```

```
ip inspect name cbac icmp                                      ②
…
interface Loopback0
  ip address 200.100.14.114 255.255.255.255
  …
  interface FastEthernet0/0.10
  …
  ip access-group eacl-in2out in                               ③
  ip inspect cbac in                                           ④
interface FastEthernet0/0.20
…
  ip access-group eacl-in2out in
  ip inspect cbac in
  …
interface Serial1/0
  ip address 200.100.15.197 255.255.255.252
  ip access-group eacl-out2in in                               ⑤
  …
ip access-list standard sacl-ssh                               ⑥
  deny 10.0.0.0 0.255.255.255
  deny 14.0.0.0 0.255.255.255
  …
  permit any
!
ip access-list extended eacl-in2out
  deny tcp any any eq 33270                                    ⑦
  deny tcp any eq 33270 any
  deny tcp any any eq 39168
  deny tcp any eq 39168 any
  deny udp any eq 1524 any
  deny udp any any eq 1524
  …
  permit ip any any                                            ⑧
ip access-list extended eacl-out2in
  deny ip 0.0.0.0 1.255.255.255 any                            ⑨
  deny ip 2.0.0.0 0.255.255.255 any
  deny ip 5.0.0.0 0.255.255.255 any
  …
  deny ip 224.0.0.0 31.255.255.255 any
  deny ip 200.100.14.0 0.0.0.127 any                           ⑩
  permit tcp any 200.100.14.112  0.0.0.7 eq 22                 ⑪
Permit tcp any host 200.100.14.126 eq smtp                     ⑫
```

```
  permit tcp any host 200.100.14.126 eq pop3                                  ⑬
  permit tcp any 200.100.14.112 0.0.0.7 range 3000 3010 time-range wkday      ⑭
  permit icmp any 200.100.14.112 0.0.0.15                                     ⑮
  deny tcp any any                                                            ⑯
  deny udp any any
  deny icmp any any                                                           ⑰
  permit ip any any                                                           ⑱
  …
line vty 0 4
  access-class sacl-ssh in                                                    ⑲
  …
  time-range wkday
  periodic weekdays 9:00 to 17:00                                             ⑳
```

配置说明如下：

①、② 配置对 TCP、UDP、ICMP 流量进行审查，这 3 条命令配合访问控制列表“eacl-out2in”实现仅允许分支机构网络到 Internet 的 TCP、UDP、ICMP 连接，禁止 Internet 到分支机构网络的主动 TCP、UDP、ICMP 连接。

③ 在边界路由器连接分支机构网络的各子接口上，配置禁止疑为 DDoS 攻击的流量入站，防御分支机构网络内主机被攻陷后主动向 Internet 外恶意用户发起的 DDoS 连接。

④ 在边界路由器连接分支机构网络的各子接口上，配置对入站 TCP、UDP、ICMP 流量进行审查。

⑤ 在边界路由器连接 Internet 的接口上，应用对入站流量进行过滤的访问控制列表“eacl-out2in”。

⑥ 该命令定义用于限制 bogon 主机使用 SSH 远程访问该边界路由器的标准 ACL，用于防御使用假冒 IP 地址对分支机构网络发动的攻击。

⑦、⑧ 定义访问控制列表“eacl-in2out”，禁止可能被 DDoS 攻击利用访问流量。

⑨、⑩ 该命令定义禁止 bogon 主机访问分支机构网络的 ACL 条目。

⑪ 该命令定义允许使用 SSH 远程管理各网络设备的 ACL 条目。

⑫、⑬ 该两条命令定义允许访问分支机构邮件服务器的 ACL 条目。

⑭ 该命令用于定义允许 Internet 在指定时间访问分支机构应用服务器 TCP 3000～3010 端口上提供的网络应用服务。

⑮ 该命令用于允许使用 ping 从 Internet 检查分支机构网络设备、服务器的联通性。

⑯、⑰ 这 3 条命令与审查命令配合，禁止 Internet 到分支机构网络主动 TCP、UDP、ICMP 连接。

⑱ 为保证路由协议等能正常工作，允许所有其他 IP 流量。

⑲ 在该边界路由器远程访问线路上应用禁止 bogon 主机访问的标准 ACL。

⑳ 为定时 ACL 条目定义的时间段“wkday”，该时间段为每周一至周五的早 9：00 到下午 5：00。

2.10 小结

作为最基础、应用最为广泛的安全控制技术,ACL在保护网络安全、防止非法入侵方面起着非常重要的作用。本章通过对模拟公司分支机构网络边界安全任务进行分析,引出对ACL知识的需求,通过对常用的几种ACL,包括基本ACL、高级ACL、定时ACL以及ASPF技术、CBAC技术的基本原理和配置方法的介绍,最终结合各种ACL实现对模拟公司分支机构网络的安全防护。

2.11 习题

1. 要求使用一条ACL规则来匹配网段202.207.120.0/24和202.207.122.0/24,请给出规则中的IP地址和通配符掩码的取值。
2. 为什么要尽量避免使用ACL的默认规则?
3. 在确定ACL的应用位置时,应遵循什么样的规则?
4. 在配置高级ACL以允许外部网络访问内部网络中的FTP服务时,为何不需要指定对FTP服务器20端口的访问允许?
5. 在ASPF的配置中,能否使用detect tcp来代替detect ftp?

2.12 实训

2.12.1 基本ACL配置实训

实验学时:2学时。

每组实验学生人数:3～4人。

1. 实验目的

掌握基本ACL的配置和验证方法。

2. 实验环境

(1) 安装有TCP/IP协议的Windows系统PC:3台

(2) 路由器:1台

(3) 二层交换机:2台

(4) UTP电缆:6条

(5) Console电缆:2条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 配置应用在接口上的基本ACL。

(2) 配置应用在VTY上的基本ACL。

4. 实验指导

(1) 按照图2-12所示的网络拓扑结构搭建网络,完成网络连接。

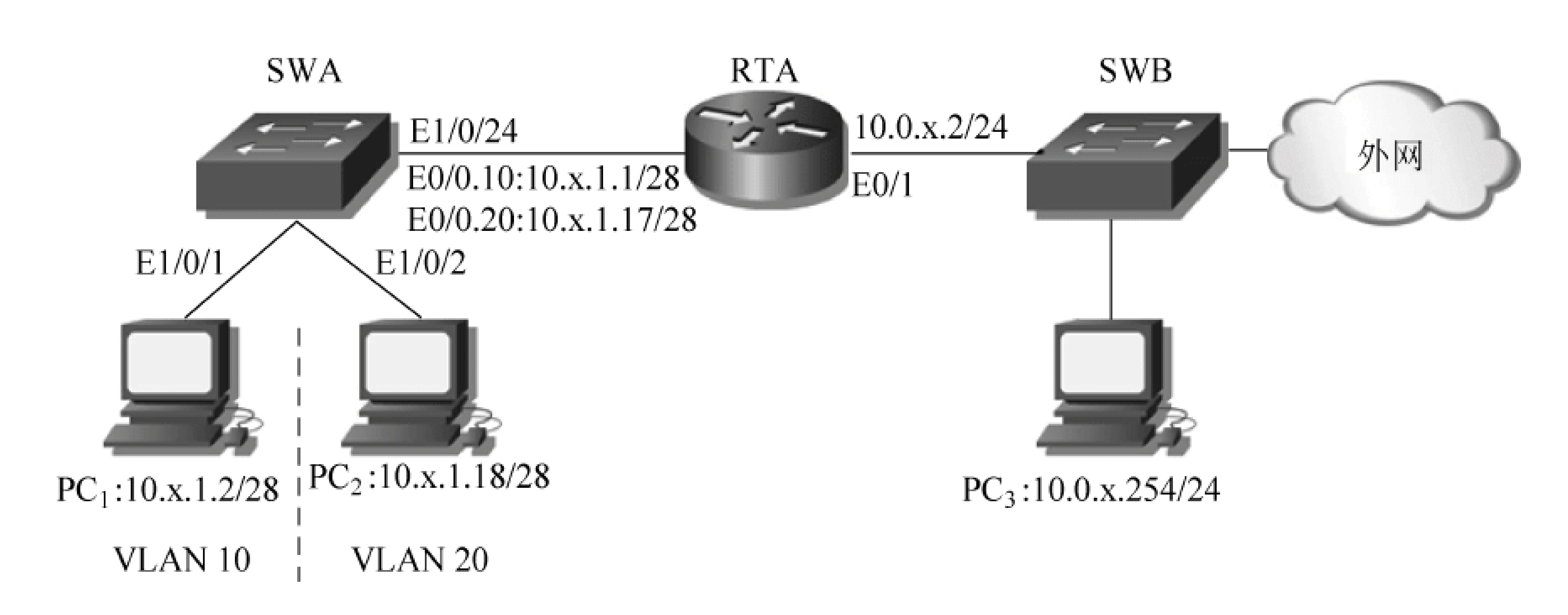


图 2-12　基本 ACL 配置实训

(2) 按照图 2-12 所示为 PC 和路由器配置 IP 地址，其中注意 PC_3 的默认网关需要设置为 10.0.x.2。交换机 SWB 保持空配置，在交换机 SWA 上划分 VLAN，在路由器 RTA 上配置单臂路由和默认路由，实现整个网络的联通性。

配置完成后，使用 ping 命令测试网络联通性，此时应保证 3 台主机之间可以通信，并且 PC_1 和 PC_2 均应能够访问外部网络。

(3) 配置基本 ACL，实现如下安全需求。

① VLAN 10 和 VLAN 20 中的主机均可以访问外部网络。

② VLAN 10 中只有 IP 地址为 10.x.1.10 的主机可以访问 VLAN 20，其他主机禁止访问 VLAN 20。

H3C 设备参考命令如下：

```
[RTA]firewall enable
[RTA]acl number 2000
[RTA-acl-basic-2000]rule permit source 10.x.1.10 0
[RTA-acl-basic-2000]rule deny source 10.x.1.0 0.0.0.15
[RTA-acl-basic-2000]rule permit
[RTA-acl-basic-2000]quit
[RTA]interface Ethernet 0/0.20
[RTA-Ethernet0/0.20]firewall packet-filter 2000 outbound
```

Cisco 设备参考命令如下：

```
RTA(config)#ip access-list standard vlan-acl
RTA(config-std-nacl)#permit host 10.x.1.10
RTA(config-std-nacl)#deny 10.x.1.0 0.0.0.15
RTA(config-std-nacl)#permit any
RTA(config-std-nacl)#exit
RTA(config)#interface FastEthernet 0/0.20
RTA(config-subif)#ip access-group vlan-acl out
```

配置完成后，在 PC_1 和 PC_2 上分别使用 ping 命令测试到达 PC_3 或外部网络任意主机的联通性，应该可以 ping 通；但在 PC_1 应该无法 ping 通 PC_2。将 PC_1 的 IP 地址修改为 10.x.1.10/28 后，PC_1 应该可以 ping 通 PC_2。

在使用 ping 命令测试的过程中,可以在路由器 RTA 上使用 display acl all 或者 show access-lists 命令查看 ACL 规则的匹配情况。

(4) 配置基本 ACL,实现如下安全需求。

内部网络主机均可以通过 VTY 方式登录到路由器 RTA 上,外部网络仅 IP 地址为 10.0.x.254 的主机可以登录,拒绝其他所有外部网络主机登录到路由器 RTA 上。

为简单起见,不再为路由器 RTA 配置专门的管理地址。

H3C 设备参考命令如下:

```
[RTA]telnet server enable
[RTA]user-interface vty 0 4
[RTA-ui-vty0-4]authentication-mode password
[RTA-ui-vty0-4]set authentication password simple network
[RTA-ui-vty0-4]user privilege level 3
[RTA-ui-vty0-4]quit
[RTA]acl number 2001
[RTA-acl-basic-2001]rule permit source 10.x.1.0 0.0.0.31
[RTA-acl-basic-2001]rule permit source 10.0.x.254 0
[RTA-acl-basic-2001]rule deny
[RTA-acl-basic-2001]quit
[RTA]user-interface vty 0 4
[RTA-ui-vty0-4]acl 2001 inbound
```

注意:ACL 2001 配置的第一条规则,使用 0.0.0.31 的通配符掩码涵盖了 VLAN 10 和 VLAN 20 两个网段。

Cisco 设备参考命令如下:

```
RTA (config)#line vty 0 4
RTA(config-line)#password network
RTA(config-line)#login
RTA(config-line)#exit
RTA(config)#ip access-list standard vty-acl
RTA(config-std-nacl)#permit 10.x.1.0 0.0.0.31
RTA(config-std-nacl)#permit host 10.0.x.254
RTA(config-std-nacl)#deny any
RTA(config-std-nacl)#exit
RTA(config)#line vty 0 4
RTA(config-line)#access-class vty-acl in
```

配置完成后,在 3 台 PC 上 Telnet 路由器 RTA 的任意一个物理接口的地址,应该可以登录(**注意**:PC_2 无法使用路由器 E0/0.10 子接口的 IP 地址 10.x.1.1 登录,因为将匹配 ACL 2000 中的规则 5),将 PC_3 的 IP 地址修改为 10.0.x.3~10.0.x.253 地址段中的任意一个 IP 地址后,将无法通过 Telnet 登录到路由器 RTA 上。

在使用 Telnet 进行测试的过程中,可以在路由器 RTA 上使用 display acl all 命令查看 ACL 规则的匹配情况。

5. 实验报告

应用在接口上的基本 ACL 配置			
应用在接口上的 ACL 测试	PC_1/PC_2 ping PC_3 或外网	是否可以 ping 通	
	PC_1 ping PC_2	是否可以 ping 通	
		匹配 ACL 规则	
	修改地址后 PC_1 ping PC_2	是否可以 ping 通	
		匹配 ACL 规则	
应用在 VTY 上的基本 ACL 配置			
应用在 VTY 上的基本 ACL 测试	PC_1/PC_2 Telnet 到 RTA	是否可以登录	
		匹配 ACL 规则	
	PC_3 Telnet 到 RTA	是否可以登录	
		匹配 ACL 规则	
	修改地址后 PC_3 Telnet 到 RTA	是否可以登录	
		匹配 ACL 规则	

2.12.2　高级 ACL 配置实训

实验学时：2 学时。

每组实验学生人数：3～4 人。

1. 实验目的

掌握高级 ACL 的配置和验证方法。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：3 台

(2) 路由器：1 台

(3) 二层交换机：1 台

(4) 三层交换机：1 台

(5) UTP 电缆：6 条

(6) Console 电缆：2 条

保持路由器和交换机均为出厂配置。

3. 实验内容

配置高级 ACL，实现网络端口级的访问控制。

4. 实验指导

(1) 按照图 2-13 所示的网络拓扑结构搭建网络，完成网络连接。

(2) 按照图 2-13 所示为路由器、三层交换机和 PC 配置 IP 地址，其中注意 PC_3 的默认网关需要设置为 10.0.x.2。交换机 SWB 保持空配置，在交换机 SWA 和路由器 RTA 上配置 RIPv2 协议以及配置默认路由，实现整个网络的联通性。

(3) 在 3 台 PC 上启动 XAMPP 软件，开启 Apache 和 FileZilla 服务，即开启 HTTP

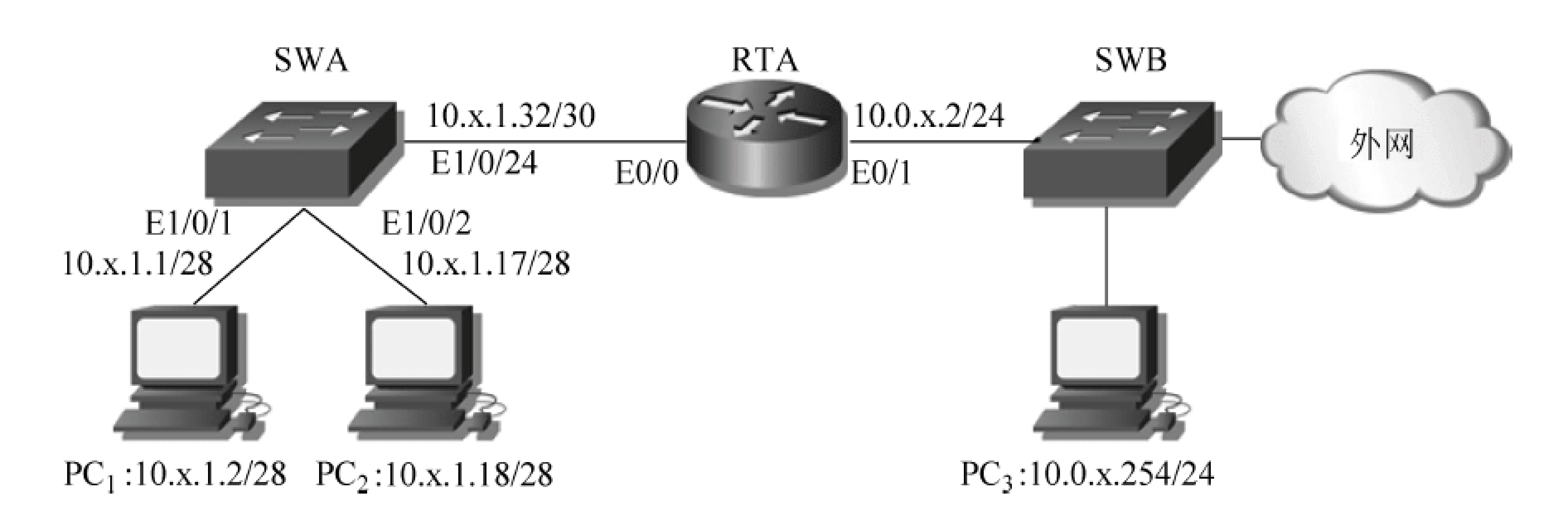


图 2-13　高级 ACL 配置实训

服务和 FTP 服务。保证 3 台 PC 之间可以互访 HTTP 和 FTP 站点。

(4) 配置高级 ACL,要求内部网络可以随意访问外部网络,而外部网络访问内部网络受到以下限制。

① 外部网络可以访问内网主机 10.x.1.2 上的 HTTP 服务。

② 外部网络可以访问内网主机 10.x.1.2 上的 FTP 服务。

③ 禁止外部网络访问其他任何关于内网的基于 TCP 的服务。

④ 禁止外部网络主动 ping 内部网络主机。

⑤ 允许其他类型的访问。

H3C 设备参考命令如下:

```
[RTA]firewall enable
[RTA]acl number 3000
[RTA-acl-adv-3000]rule permit tcp destination 10.x.1.2 0 destination-port eq 80
[RTA-acl-adv-3000]rule permit tcp destination 10.x.1.2 0 destination-port eq 20
[RTA-acl-adv-3000]rule permit tcp destination 10.x.1.2 0 destination-port eq 21
[RTA-acl-adv-3000]rule permit tcp established
[RTA-acl-adv-3000]rule deny tcp
[RTA-acl-adv-3000]rule deny icmp icmp-type echo
[RTA-acl-adv-3000]rule permit ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall packet-filter 3000 inbound
```

Cisco 设备参考命令如下:

```
RTA(config)#ip access-list extended out2in
RTA(config-ext-nacl)#permit tcp any host 10.x.1.2 eq 80
RTA(config-ext-nacl)#permit tcp any host 10.x.1.2 eq 20
RTA(config-ext-nacl)#permit tcp any host 10.x.1.2 eq 21
RTA(config-ext-nacl)#permit tcp any any established
RTA(config-ext-nacl)#deny tcp any any
RTA(config-ext-nacl)#deny icmp any any echo
RTA(config-ext-nacl)#permit ip any any
RTA(config-ext-nacl)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip access-group out2in in
```

配置完成后，在 PC_1 和 PC_2 上分别使用 ping 命令测试到达 PC_3 或外部网络任意主机的联通性，应该可以 ping 通；但是在 PC_3 上使用 ping 命令测试到达 PC_1 和 PC_2 的联通性，应该无法 ping 通。

在 PC_1 和 PC_2 上应该可以访问 PC_3 上的 HTTP 和 FTP 服务；在 PC_3 上应该无法访问 PC_2 上的 HTTP 和 FTP 服务；在 PC_3 上应该可以访问 PC_1 上的 HTTP 服务；在默认的被动模式下，PC_3 上应该无法访问 PC_1 上的 FTP 服务；将 PC_3 的 FTP 连接模式修改为主动模式后，PC_3 上应该可以访问 PC_1 上的 FTP 服务。

在进行测试的过程中，可以在路由器 RTA 上使用 display acl all 或 show access-lists 命令查看 ACL 规则的匹配情况。

(5) 将 ACL 中的第 2 条规则，即允许外部网络访问内网主机 10.x.1.2 上的 FTP 数据端口的规则删除。

H3C 设备参考命令如下：

```
[RTA]acl number 3000
[RTA-acl-adv-3000]undo rule 5
```

Cisco 设备参考命令如下：

```
RTA(config)#ip access-list extended out2in
RTA(config-ext-nacl)#no permit tcp any host 10.x.1.2 eq 20
```

配置完成后，测试在 PC_3 上使用主动模式是否还可以访问 PC_1 上的 FTP 服务，并解释原因。

测试结果应该是 PC_3 依然可以访问 PC_1 上的 FTP 服务。因为在主动模式下，FTP 的数据连接将由 FTP 服务器即内网主机 10.x.1.2 发起，而由外部网络主机 PC_3 进行响应，此时从外部网络进入内网的数据连接流量将匹配规则 rule permit tcp established，从而被允许。

5. 实验报告

高级 ACL 配置			
高级 ACL 测试	PC_1/PC_2 ping PC_3 或外网	是否可以 ping 通	
		匹配 ACL 规则	
	PC_3 ping PC_1/PC_2	是否可以 ping 通	
		匹配 ACL 规则	
	PC_1/PC_2 访问 PC_3 的 HTTP/FTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 访问 PC_2 的 HTTP/FTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 访问 PC_1 的 HTTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 使用主动模式访问 PC_1 的 FTP 服务	是否可以访问	
		匹配 ACL 规则	
	删除 rule 5 后 PC_3 使用主动模式访问 PC_1 的 FTP 服务	是否可以访问	
		解释原因	

2.12.3 ASPF/CBAC 配置实训

实验学时：2学时。

每组实验学生人数：3～4人。

1. 实验目的

掌握 ASPF/CBAC 的配置和验证方法。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：3台

(2) 路由器：1台

(3) 二层交换机：1台

(4) 三层交换机：1台

(5) UTP 电缆：6条

(6) Console 电缆：2条

保持路由器和交换机均为出厂配置。

3. 实验内容

配置 ASPF/CBAC,通过 TACL 和静态 ACL 的组合实现精确访问控制策略。

4. 实验指导

注意：本次实验是实验2.12.2的延续,应在正确完成实验2.12.2的基础上进行本次实验。

(1) 分析实验2.12.2存在的问题。作为静态的 ACL 形式,虽然高级 ACL 可以实现网络端口级的访问控制,但无法对网络中的流量进行监控。在实验2.12.2中,为保证内部网络主机可以访问外部网络的基于 TCP 的服务,配置了规则 rule permit tcp established,但该规则可能会导致伪造 TCP 响应报文的攻击；另外,实验2.12.2也无法防范基于 UDP 的攻击。

(2) 配置 ASPF/CBAC 策略与高级 ACL 相配合,实现以下安全需求。

① 外部网络可以访问内网主机10.x.1.2上的 HTTP 服务。

② 外部网络可以访问内网主机10.x.1.2上的 FTP 服务。

③ 禁止外部网络访问其他任何关于内网的基于 TCP 的服务。

④ 禁止外部网络访问任何关于内网的基于 UDP 的服务。

⑤ 禁止外部网络主动 ping 内部网络主机。

⑥ 允许其他类型的访问。

从安全需求上看,和实验2.12.2的区别仅仅是多了第4条关于 UDP 的限制,但是在实现上将存在较大区别。

H3C 设备参考命令如下：

```
[RTA]acl number 3000
[RTA-acl-adv-3000]undo rule 15
[RTA-acl-adv-3000]rule 15 deny udp
[RTA-acl-adv-3000]quit
[RTA]aspf-policy 1
```

```
[RTA-aspf-policy-1]detect ftp
[RTA-aspf-policy-1]detect tcp
[RTA-aspf-policy-1]detect udp
[RTA-aspf-policy-1]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall aspf 1 outbound
```

注意：在此将在实验 2.12.2 中配置 ACL 3000 的规则进行了修改，修改后的 ACL 3000 的规则如下：

```
[RTA]display acl 3000
Advanced ACL  3000, named -none-, 6 rules,
ACL's step is 5
  rule 0 permit tcp destination 10.9.1.2 0 destination-port eq www
  rule 10 permit tcp destination 10.9.1.2 0 destination-port eq ftp
  rule 15 deny udp
  rule 20 deny tcp
  rule 25 deny icmp icmp-type echo
  rule 30 permit ip
```

从规则中可以看出，除了对于 10.9.1.2 的 HTTP 和 FTP 服务的访问，实际上拒绝了所有从外部网络到内部网络的 TCP 和 UDP 流量。

在 ASPF 策略的审查规则中，单通道应用层协议 HTTP 使用 TCP 协议检测即可，而多通道应用层协议 FTP 需要单独配置检测。

Cisco 设备参考命令如下：

```
RTA(config)#ip access-list extended out2in
RTA(config-ext-nacl)#no permit tcp any any established
RTA(config-ext-nacl)#no permit ip any any
RTA(config-ext-nacl)#deny udp any any
RTA(config-ext-nacl)#permit ip any any
RTA(config)#ip inspect name network ftp
RTA(config)#ip inspect name network tcp
RTA(config)#ip inspect name network udp
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip inspect network out
```

修改后的扩展 ACL out2in 的规则如下：

```
RTA#show access-lists out2in
Extended IP access list out2in
    permit tcp any host 10.1.1.2 eq www
    permit tcp any host 10.1.1.2 eq ftp
    deny tcp any any
    deny icmp any any echo
    deny udp any any
    permit ip any any
```

配置完成后，进行相关测试，ping 命令测试结果与 ACL 匹配情况与实验 2.12.2 完

全相同,在此不再赘述。

在 PC_1 和 PC_2 上可以访问 PC_3 上的 HTTP 和 FTP 服务;在 PC_3 上无法访问 PC_2 上的 HTTP 和 FTP 服务;在 PC_3 上可以访问 PC_1 上的 HTTP 服务;在默认的被动模式下,PC_3 上无法访问 PC_1 上的 FTP 服务;将 PC_3 的 FTP 连接模式修改为主动模式后,PC_3 上可以访问 PC_1 上的 FTP 服务。

注意:本部分测试结果与实验 2.12.2 完全相同,但是匹配的规则与实验 2.12.2 有所区别。

在进行测试的过程中,可以在路由器 RTA 上使用 display acl all 或者 show access-lists 命令查看 ACL 规则的匹配情况,使用 display aspf session 或者 show ip inspect sessions 命令查看 ASPF 的会话信息。

5. 实验报告

高级 ACL 配置			
ASPF/CBAC 策略配置			
高级 ACL 及 ASPF/CBAC 测试	PC_1/PC_2 访问 PC_3 的 HTTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_1/PC_2 访问 PC_3 的 FTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_3 访问 PC_2 的 HTTP/FTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 访问 PC_1 的 HTTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 使用主动模式访问 PC_1 的 FTP 服务	是否可以访问	
		匹配 ACL 规则	
		匹配 ASPF/CBAC 规则	

2.12.4 ACL 综合应用实训 1

实验学时:4 学时。

每组实验学生人数:3~4 人。

1. 实验目的

掌握在网络中综合应用 ACL 和 ASPF/CBAC 实现访问控制的能力。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC:4 台

(2) 路由器:2 台

(3) 二层交换机:2 台

(4) V.35 背对背电缆:1 条

(5) UTP 电缆:7 条

(6) Console 电缆:2 条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 配置高级 ACL。

(2) 配置 ASPF/CBAC。

4. 实验指导

(1) 按照图 2-14 所示的网络拓扑结构搭建网络,完成网络连接。

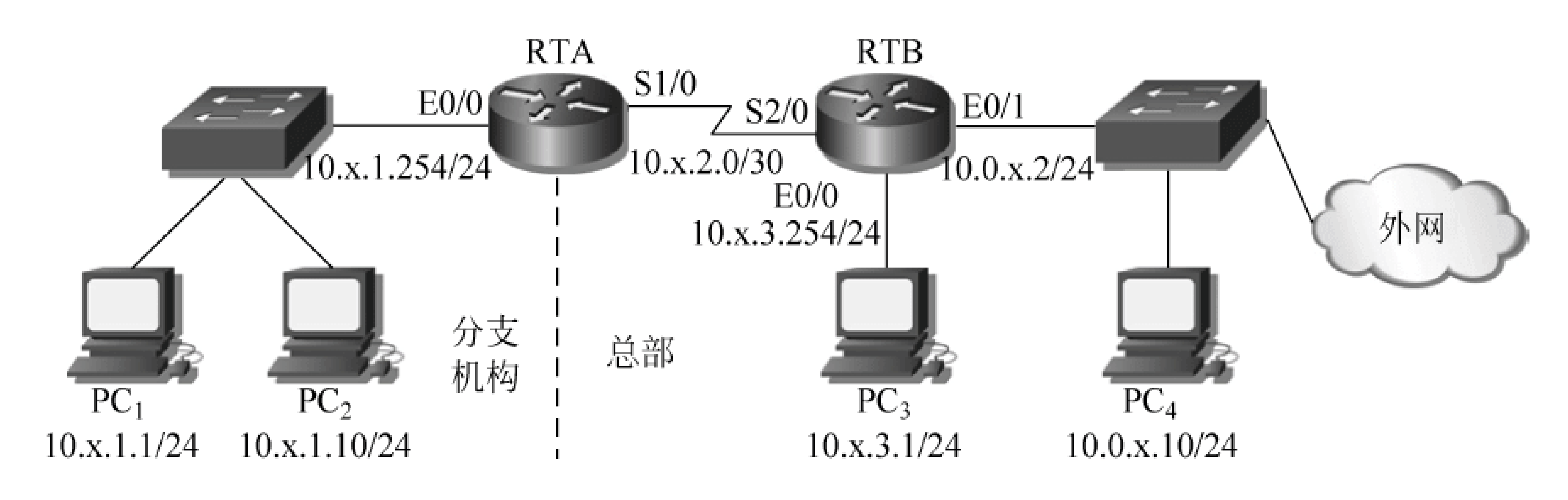


图 2-14　ACL 综合应用实训 1

(2) 按照图 2-14 所示为路由器和 PC 配置 IP 地址,其中注意 PC_4 的默认网关需要设置为 10. 0. x. 2。两台交换机均保持空配置,在路由器 RTA 和 RTB 上配置 RIPv2 协议以及配置默认路由,实现整个网络的联通性。

(3) 在 PC_3 和 PC_4 上启动 XAMPP 软件,开启 Apache 和 FileZilla 服务,即开启 HTTP 服务和 FTP 服务。保证另外 3 台主机均可访问 PC_3 和 PC_4 的 HTTP 和 FTP 站点。

(4) 配置高级 ACL 和 ASPF/CBAC,实现以下安全需求。

① 分支机构网络可以任意访问总部网络和外部网络,总部网络可以任意访问外部网络,包括各种基于 TCP 和 UDP 的服务。

② 总部网络只能访问分支机构网络中的 IP 地址为 10. x. 1. 1～10. x. 1. 7 的主机,不能访问分支机构网络中的其他主机。

③ 外部网络主机可以访问总部网络中 PC_3 上的 HTTP 服务和 FTP 服务,但不能访问总部网络上的其他主机。

④ 外部网络主机可以访问分支机构网络中除 IP 地址为 10. x. 1. 1～10. x. 1. 7 以外的主机。

H3C 设备参考命令如下:

```
[RTA]firewall enable
[RTA]aspf-policy 1
[RTA-aspf-policy-1]detect ftp
[RTA-aspf-policy-1]detect tcp
[RTA-aspf-policy-1]detect udp
[RTA-aspf-policy-1]quit
[RTA]interface Serial 1/0
[RTA-Serial1/0]firewall aspf 1 outbound
[RTA-Serial1/0]quit
```

```
[RTA]acl number 3000
[RTA-acl-adv-3000]rule permit ip destination 10.x.1.0 0.0.0.7
[RTA-acl-adv-3000]rule permit icmp icmp-type echo-reply
[RTA-acl-adv-3000]rule deny ip source 10.x.3.0 0.0.0.255 destination 10.x.1.0 0.0.0.255
[RTA-acl-adv-3000]rule permit ip
[RTA-acl-adv-3000]quit
[RTA]interface Serial 1/0
[RTA-Serial1/0]firewall packet-filter 3000 inbound

[RTB]firewall enable
[RTB]aspf-policy 2
[RTB-aspf-policy-2]detect ftp
[RTB-aspf-policy-2]detect tcp
[RTB-aspf-policy-2]detect udp
[RTB-aspf-policy-2]quit
[RTB]interface Ethernet 0/1
[RTB-Ethernet0/1]firewall aspf 2 outbound
[RTB-Ethernet0/1]quit
[RTB]acl number 3001
[RTB-acl-adv-3001]rule permit tcp destination 10.x.3.1 0 destination-port eq 80
[RTB-acl-adv-3001]rule permit tcp destination 10.x.3.1 0 destination-port eq 21
[RTB-acl-adv-3001]rule permit icmp icmp-type echo-reply
[RTB-acl-adv-3001]rule deny ip destination 10.x.3.0 0.0.0.255
[RTB-acl-adv-3001]rule deny ip destination 10.x.1.0 0.0.0.7
[RTB-acl-adv-3001]rule permit ip
[RTB-acl-adv-3001]quit
[RTB]interface Ethernet 0/1
[RTB-Ethernet0/1]firewall packet-filter 3001 inbound
```

在进行 ACL 配置时,一定要注意分别在两台路由器上配置的 ACL 规则之间的关联,因为在本次实验中,从外部网络访问分支机构网络需要在路由器 RTB 的 Ethernet 0/1 接口的 inbound 方向上和路由器 RTA 的 Serial 1/0 接口的 inbound 方向上进行两次 ACL 规则的匹配。对于外部网络允许进入分支机构网络的流量一定要保证两次匹配均为 permit 才行。例如,外部网络主机 PC_4 对分支机构网络中 PC_2 的访问,在路由器 RTB 上匹配规则 rule permit ip,在路由器 RTA 上同样匹配规则 rule permit ip,因此 PC_4 可以访问 PC_2。进一步分析发现,在安全需求中第二条要求和第四条要求实际上完全相反,为保证外部网络对分支机构网络中除 IP 地址为 10.x.1.1～10.x.1.7 以外的主机访问,在路由器 RTA 上满足第二条要求的规则只能写成 rule deny ip source 10.x.3.0 0.0.0.255 destination 10.x.1.0 0.0.0.255,即需要做源 IP 地址的精确匹配,如果该条规则写成了 rule deny ip destination 10.x.1.0 0.0.0.255,则会导致外部网络主机访问分支机构网络的正常流量被拒绝。

Cisco 设备参考命令如下:

```
RTA(config)#ip inspect name syn1 ftp
RTA(config)#ip inspect name syn1 tcp
RTA(config)#ip inspect name syn1 udp
```

```
RTA(config)#interface Serial 0/0
RTA(config-if)#ip inspect syn1 out
RTA(config-if)#exit
RTA(config)#ip access-list extended out2in1
RTA(config-ext-nacl)#permit ip any 10.x.1.0 0.0.0.7
RTA(config-ext-nacl)#permit icmp any any echo-reply
RTA(config-ext-nacl)#deny ip 10.x.3.0 0.0.0.255 10.x.1.0 0.0.0.255
RTA(config-ext-nacl)#permit ip any any
RTA(config-ext-nacl)#exit
RTA(config)#interface Serial 0/0
RTA(config-if)#ip access-group out2in1 in

RTB(config)#ip inspect name syn2 ftp
RTB(config)#ip inspect name syn2 tcp
RTB(config)#ip inspect name syn2 udp
RTB(config)#interface FastEthernet 0/1
RTB(config-if)#ip inspect syn2 out
RTB(config-if)#exit
RTB(config)#ip access-list extended out2in2
RTB(config-ext-nacl)#permit tcp any host 10.x.3.1 eq 80
RTB(config-ext-nacl)#permit tcp any host 10.x.3.1 eq 21
RTB(config-ext-nacl)#permit icmp any any echo-reply
RTB(config-ext-nacl)#deny ip any 10.x.3.0 0.0.0.255
RTB(config-ext-nacl)#deny ip any 10.x.1.0 0.0.0.7
RTB(config-ext-nacl)#permit ip any any
RTB(config-ext-nacl)#exit
RTB(config)#interface FastEthernet 0/1
RTB(config-if)#ip access-group out2in2 in
```

配置完成后，进行如下相关测试。

在分支机构网络主机 PC_1 和 PC_2 上使用 ping 命令测试到达总部网络主机 PC_3 和外部网络主机 PC_4 的联通性，都可以 ping 通；总部网络主机 PC_3 可以 ping 通外部网络主机 PC_4。

在分支机构网络主机 PC_1 和 PC_2 上可以访问总部网络主机 PC_3 和外部网络主机 PC_4 上的 HTTP 和 FTP 服务；在总部网络主机 PC_3 上可以访问外部网络主机 PC_4 上的 HTTP 和 FTP 服务。

在总部网络主机 PC_3 上可以 ping 通分支机构网络主机 PC_1，无法 ping 通分支机构网络主机 PC_2。

在外部网络主机 PC_4 上应该可以访问总部网络主机 PC_3 上的 HTTP 服务，在外部网络主机 PC_4 上应该可以使用主动模式访问总部网络主机 PC_3 上的 FTP 服务；将 PC_3 的 IP 地址更改为 10.x.3.2～10.x.3.253 区段中的任何一个地址后，PC_4 应该将无法访问 PC_3 上的 HTTP 和 FTP 服务。

在外部网络主机 PC_4 上无法 ping 通分支机构网络主机 PC_1，可以 ping 通分支机构网络主机 PC_2。

5. 实验报告

RTA 上高级 ACL 配置			
RTA 上 ASPF 策略配置			
RTB 上高级 ACL 配置			
RTB 上 ASPF 策略配置			
高级 ACL 及 ASPF 测试	PC_1/PC_2 访问 PC_3 的 HTTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_1/PC_2 访问 PC_3 的 FTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_3 访问 PC_4 的 HTTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_3 访问 PC_4 的 FTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_3 ping PC_1	是否可以 ping 通	
		匹配 ACL 规则	
	PC_3 ping PC_2	是否可以 ping 通	
		匹配 ACL 规则	
	PC_4 访问 PC_3 的 HTTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_4 使用主动模式访问 PC_3 的 FTP 服务	是否可以访问	
		匹配 ACL 规则	
		匹配 ASPF/CBAC 规则	
	PC_4 ping PC_1	是否可以 ping 通	
		匹配 ACL 规则	
	PC_4 ping PC_2	是否可以 ping 通	
		匹配 ACL 规则	

2.12.5 ACL 综合应用实训 2

实验学时：2 学时。

每组实验学生人数：3～4 人。

1. 实验目的

掌握在网络中综合应用 ACL 和 ASPF/CBAC 实现访问控制的能力。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：3 台

(2) 路由器：2 台

(3) 二层交换机：1 台

(4) UTP 电缆：6 条

(5) Console 电缆：2 条

保持路由器和交换机均为出厂配置。

3. 实验内容

（1）配置高级 ACL。

（2）配置 ASPF/CBAC。

4. 实验指导

（1）按照图 2-15 所示的网络拓扑结构搭建网络，完成网络连接。

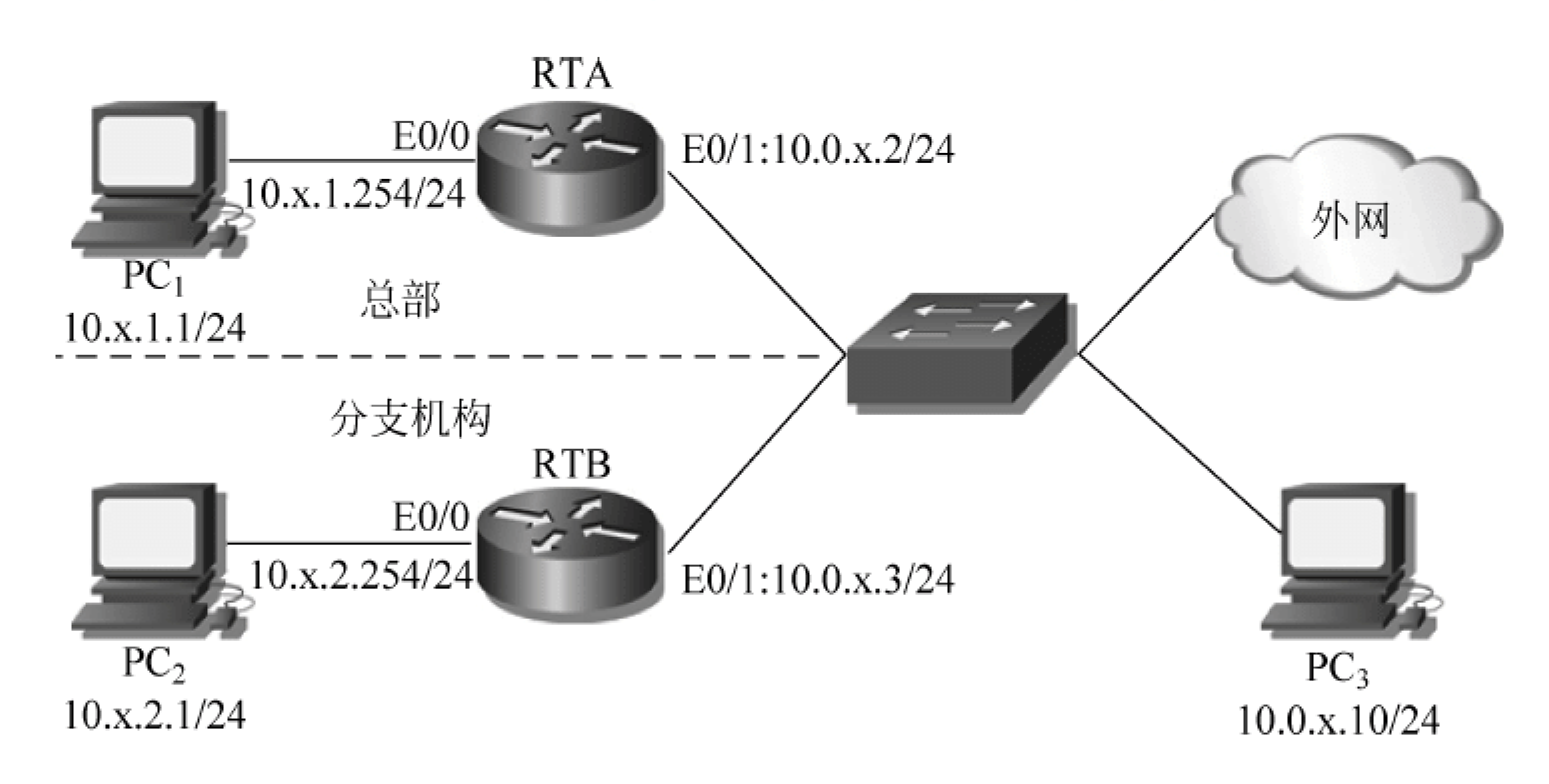


图 2-15　ACL 综合应用实训 2

（2）按照图 2-15 所示为路由器和 PC 配置 IP 地址，其中注意 PC_3 的默认网关要根据具体的网络测试需求进行设置，具体见配置完成后的测试部分的要求。交换机保持空配置，在路由器 RTA 和 RTB 上配置 RIPv2 协议以及配置默认路由，实现整个网络的联通性。

（3）在 PC_1 和 PC_3 上启动 XAMPP 软件，开启 Apache 和 FileZilla 服务，即开启 HTTP 服务和 FTP 服务。保证另外两台主机均可访问 PC_1 和 PC_3 的 HTTP 和 FTP 站点。

（4）配置高级 ACL 和 ASPF/CBAC，实现以下安全需求。

① 分支机构网络可以随意访问总部网络和外部网络，包括各种基于 TCP 和 UDP 的服务。但总部网络和外部网络均无法主动访问分支机构网络。限于分支机构网络的出口路由器 RTB 的性能问题，不能在其上配置 ASPF。

② 总部网络可以任意访问外部网络，包括各种基于 TCP 和 UDP 的服务。

③ 外部网络主机可以访问总部网络中 PC_1 上的 HTTP 服务和 FTP 服务，但不能访问总部网络上的其他主机。

H3C 设备参考命令如下：

```
[RTA]firewall enable
[RTA]aspf-policy 1
[RTA-aspf-policy-1]detect ftp
[RTA-aspf-policy-1]detect tcp
[RTA-aspf-policy-1]detect udp
[RTA-aspf-policy-1]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall aspf 1 outbound
```

```
[RTA-Ethernet0/1]quit
[RTA]acl number 3000
[RTA-acl-adv-3000]rule permit tcp destination 10.x.1.1 0 destination-port eq 80
[RTA-acl-adv-3000]rule permit tcp destination 10.x.1.1 0 destination-port eq 21
[RTA-acl-adv-3000]rule permit icmp icmp-type echo-reply
[RTA-acl-adv-3000]rule permit udp destination 224.0.0.9 0 destination-port eq 520
[RTA-acl-adv-3000]rule permit ip source 10.x.2.0 0.0.0.255 destination 10.x.1.0 0.0.0.255
[RTA-acl-adv-3000]rule deny ip
[RTA-acl-adv-3000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]firewall packet-filter 3000 inbound

[RTB]firewall enable
[RTB]acl number 3001
[RTB-acl-adv-3001]rule permit tcp established
[RTB-acl-adv-3001]rule deny tcp
[RTB-acl-adv-3001]rule deny icmp icmp-type echo
[RTB-acl-adv-3001]rule permit ip
[RTB-acl-adv-3001]quit
[RTB]interface Ethernet 0/1
[RTB-Ethernet0/1]firewall packet-filter 3001 inbound
```

注意:在路由器 RTA 上配置的 ACL 3000 中的第 4 条规则 rule permit udp destination 224.0.0.9 0 destination-port eq 520,本条规则是允许路由器 RTA 接收来自路由器 RTB 的路由更新,如果没有该条规则,则将导致路由器 RTA 无法获知去往分支机构网络 10.x.2.0/24 的路由。

Cisco 设备参考命令如下:

```
RTA(config)#ip inspect name syn1 ftp
RTA(config)#ip inspect name syn1 tcp
RTA(config)#ip inspect name syn1 udp
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip inspect syn1 out
RTA(config-if)#exit
RTA(config)#ip access-list extended in2out1
RTA(config-ext-nacl)#permit tcp any host 10.x.1.1 eq 80
RTA(config-ext-nacl)#permit tcp any host 10.x.1.1 eq 21
RTA(config-ext-nacl)#permit icmp any any echo-reply
RTA(config-ext-nacl)#permit udp any host 224.0.0.9 eq 520
RTA(config-ext-nacl)#permit ip 10.x.2.0 0.0.0.255 10.x.1.0 0.0.0.255
RTA(config-ext-nacl)#deny ip any any
RTA(config-ext-nacl)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip access-group out2in1 in

RTB(config)#ip access-list extended out2in2
RTB(config-ext-nacl)#permit tcp any any established
RTB(config-ext-nacl)#deny tcp any any
RTB(config-ext-nacl)#deny icmp any any echo
```

```
RTB(config-ext-nacl)#permit ip any any
RTB(config-ext-nacl)#exit
RTB(config)#interface FastEthernet 0/1
RTB(config-if)#ip access-group out2in2 in
```

配置完成后，进行如下相关测试。

首先将 PC_3 的默认网关设置为 10.0.x.3，在分支机构网络主机 PC_2 上使用 ping 命令测试到达总部网络主机 PC_1 和外部网络主机 PC_3 的联通性，都可以 ping 通；但是从总部网络主机 PC_1 上无法 ping 通分支机构网络主机 PC_2，从外部网络主机 PC_3 应该也无法 ping 通分支机构网络主机 PC_2。

在分支机构网络主机 PC_2 上可以访问总部网络主机 PC_1 和外部网络主机 PC_3 上的 HTTP 和 FTP 服务。

将 PC_3 的默认网关设置为 10.0.x.2，在总部网络主机 PC_1 上可以访问外部网络主机 PC_3 上的 HTTP 和 FTP 服务。

在外部网络主机 PC_3 上可以访问总部网络主机 PC_1 上的 HTTP 服务，在外部网络主机 PC_3 上可以使用主动模式访问总部网络主机 PC_1 上的 FTP 服务；将 PC_1 的 IP 地址更改为 10.x.1.2～10.x.1.253 区段中的任何一个地址后，PC_3 将无法访问 PC_1 上的 HTTP 和 FTP 服务。

注意对于外部网络主机 PC_3 默认网关的设置，在没有配置任何安全策略的情况下，PC_3 的默认网关设置为 10.0.x.2 或 10.0.x.3 都可以，只是在访问有些网络的时候，路由会多一跳。例如，将 PC_3 的默认网关设置为 10.0.x.3，则 PC_3 在访问总部网络主机 PC_1 时的路由为 PC_3—RTB—RTA—PC_1，比默认网关设置为 10.0.x.2 时的路由 PC_3—RTA—PC_1 多了 RTB 这一跳。但是在配置了安全策略后，则有可能会出现正常访问流量被拒绝的情况。在此，依然由 PC_3 访问总部网络主机 PC_1 的 HTTP 或者 FTP 服务，如果默认网关设置为 10.0.x.3，则 PC_3 的流量首先送到路由器 RTB，在 RTB 接口 Ethernet 0/1 的 inbound 方向上会匹配规则 rule deny tcp，从而导致流量被拒绝，但将 PC_3 的默认网关设置为 10.0.x.2 则不会有问题。反之亦然，这就是为什么在测试时需要更改 PC_3 的默认网关的原因。

5. 实验报告

RTA 上高级 ACL 配置			
RTA 上 ASPF/CBAC 策略配置			
RTB 上高级 ACL 配置			
高级 ACL 及 ASPF/CBAC 测试	PC_2 ping PC_1	是否可以 ping 通	
		匹配 ACL 规则	
	PC_2 ping PC_3	是否可以 ping 通	
		匹配 ACL 规则	
	PC_1/PC_3 ping PC_2	是否可以 ping 通	
		匹配 ACL 规则	

续表

高级 ACL 及 ASPF/CBAC 测试	PC_2 访问 PC_1 上的 HTTP/FTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_2 访问 PC_3 上的 HTTP/FTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_1 访问 PC_3 上的 HTTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_1 访问 PC_3 上的 FTP 服务	是否可以访问	
		匹配 ASPF/CBAC 规则	
	PC_3 访问 PC_1 的 HTTP 服务	是否可以访问	
		匹配 ACL 规则	
	PC_3 使用主动模式访问 PC_1 的 FTP 服务	是否可以访问	
		匹配 ACL 规则	
		匹配 ASPF/CBAC 规则	

第 3 章

网络地址转换

本章任务：根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题。

必备知识：(1) 静态 NAT。

(2) NAPT。

(3) 端口地址重定向。

学习目标：完成模拟公司分支机构网络内外网地址转换配置任务，解决公司内网地址资源不足问题。

3.1 模拟公司分支机构网络地址转换任务分析

由表 2-9 所示的模拟公司 IP 地址分配情况可知，分支机构 B-1 可用的公共 IP 地址仅有 62 个，但随着该分支机构业务发展，网络不断扩大，所分配公共 IP 地址出现不足。为解决 IP 地址紧张问题，模拟公司分支机构 B-1 网络内准备使用私有地址 10.0.0.0/24 替换原网络中的公共 IP 地址。但使用私有地址的分支机构网络不能与分支机构以外的网络通信，为满足分支机构网络以下通信要求，必须使用地址转换技术对进出分支机构网络的报文进行地址转换。

(1) 分支机构 B-1 内部网络中服务器 Ser1 向外网同时提供网站、邮件服务，同时 1 台"独立的"Web 服务器 WebSer1 和 1 台独立的邮件服务器 MailSer1 也同时向外网提供服务。

(2) 分支机构 8 名主管的办公用机需要访问网络上的多媒体服务。

(3) 分支机构 B-1 内部网络中 200 台主机要能访问 Internet 资源。

(4) 分支机构 B-1 在其网络内部模拟公司总部生产网搭建了一套生产系统，该模拟生产系统在分支机构网络内使用了与总部相同的网络地址 200.100.11.0/24，但该生产系统有时需要访问总部生产网下载部分生产数据用于分析研究。

(5) 尽可能节省公共 IP 地址。

表 3-1 显示了分支机构 B-1 内各主机使用 IP 地址情况。

表 3-1　分支机构 B-1 IP 地址分配情况

序号	内网主机	内部本地地址/网络前缀	网关地址
1	模拟生产系统	10.0.0.0/28	10.0.0.14
2	Ser1	10.0.0.17/28	10.0.0.30
3	WebSer1	10.0.0.18/28	10.0.0.30
4	MailSer1	10.0.0.19/28	10.0.0.30
5	普通主机	10.0.2.0/24	10.0.2.254
6	主管用机	10.0.3.0/24	10.0.3.254

3.2　网络地址转换的基本概念

网络地址转换(Network Address Translation,NAT)技术最初是作为缓解 IPv4 地址空间紧张的一种解决方案引入的,其主要作用就是通过将私有 IP 地址转换为合法的公有 IP 地址,使私有网络中的主机可以通过共享少量的公有 IP 地址访问 Internet。随着网络的爆炸性增长,IPv4 的地址空间变得非常紧张,租用公有 IP 地址也变得非常困难和昂贵,因此企业在组建自己的私有网络时,通常会在企业内部网络中使用 RFC1918 定义的私有 IP 地址(10.0.0.0/8、172.16.0.0/12、192.168.0.0/16),而在企业内部网络主机有访问 Internet 需求时,在企业的边界网关路由器上使用 NAT 技术将私有 IP 地址转换到租用的少量公有 IP 地址上,从而使用少量的公有 IP 地址来满足企业连接 Internet 的需求。

除了可以缓解 IPv4 地址空间的紧张外,NAT 技术在客观上屏蔽了企业内部网络的真实 IP 地址,一定程度上保护了内部网络不受到外部网络的主动攻击。例如,在使用动态 NAT 技术进行地址转换时,内部网络主机可以访问外部网络主机,但外部网络主机将无法主动访问内部网络中的主机,因此也提高了企业内部网络的安全性。

3.2.1　网络地址转换的工作过程

网络地址转换一般在网络的边界由网络地址转换设备实现,例如配置了地址转换功能的路由器或防火墙。网络地址转换设备使用地址转换表保存私有 IP 地址和公有 IP 地址的映射关系,并根据保存的映射关系对 IP 地址进行转换。典型的网络地址转换过程如图 3-1 所示。

在 PC_1 访问外部网络主机时,其产生的数据报文的源 IP 地址是 PC_1 在内部网络的私有 IP 地址(内部本地地址)192.168.1.10,当数据报文到达出口路由器的出接口时,路由器将数据报文的源 IP 地址转换为内部全局地址 202.207.120.10,使数据报文可以在公共网络上路由,并将内部本地地址和内部全局地址的映射关系保存在地址转换表中;在返回的数据报文中,目的 IP 地址为内部全局地址 202.207.120.10,在路由器接收到该报文后,根据地址转换表中保存的映射关系将目的 IP 地址转换为内部本地地址 192.168.1.10,并路由给内部网络的目的主机 PC_1,从而实现 PC_1 和外部网络主机之间的通信。

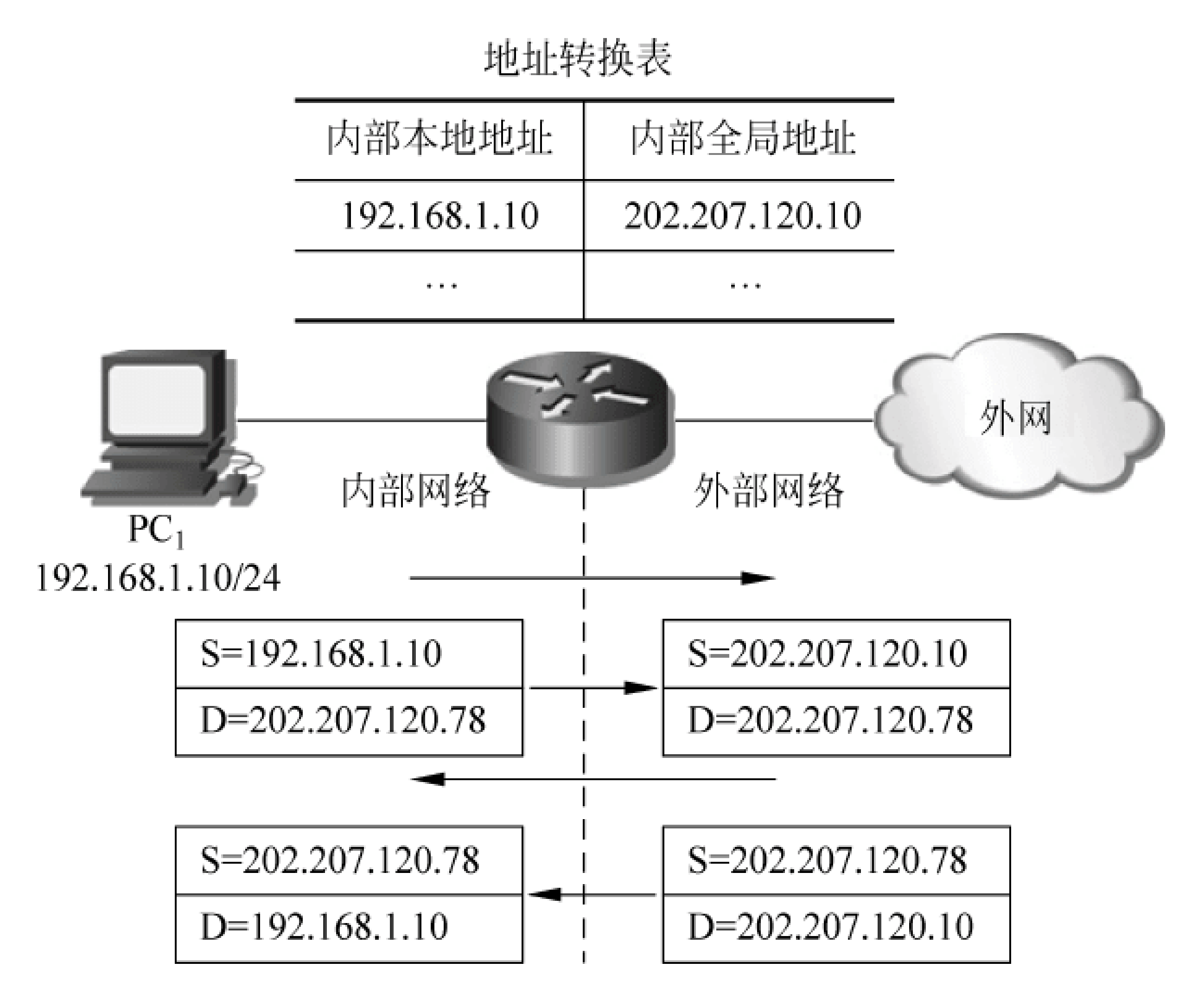


图 3-1　网络地址转换过程

注意：上面给出的只是一个典型的网络地址转换过程，实际上不同类型的网络地址转换在处理上会有所区别。

3.2.2　网络地址转换的类型

按照网络地址转换对象的不同，可以将网络地址转换分为内部网络地址转换和外部网络地址转换两种。其中外部网络地址转换主要用于内外网使用的 IP 地址重叠时，即内部网络随意使用了合法公有 IP 地址时，将外部网络主机与内部网络主机重叠的公有 IP 地址(外部全局地址)在内部网络转换为外部本地地址，由于相对应用比较少，因此在本书中不再进行介绍。

内部网络地址转换按照地址转换的原理、转换方式以及应用场合的不同可以划分为如表 3-2 所示的 5 种。

表 3-2　网络地址转换类型

网络地址转换类型	说　　明
静态网络地址转换	手工配置本地地址到全局地址的一对一的映射，适用于需要固定全局 IP 地址的内网服务器
动态网络地址转换	本地地址到全局地址为一对一映射，但映射关系不固定，本地地址共享地址池中的全局地址
网络地址端口转换	本地地址到全局地址使用端口号实现动态的多对一映射，可显著提高全局地址的利用率，又称为地址的过载
基于接口的地址转换	网络地址端口转换的特殊形式，又称为 Easy IP。与网络地址端口转换的区别是本地地址均映射到出口路由器的出接口地址上
端口地址重定向	又称为 NAT Server，手工配置“本地地址＋端口”到“全局地址＋端口”的一对一的映射。适用于多台内网服务器映射到一个全局地址的情况

使用哪一种网络地址转换技术来进行地址的转换需要根据网络的具体需求来确定。很多时候在同一个网络中可能会涉及多种网络地址转换技术。例如,某一企业中大量的内部网络主机都有访问 Internet 的需求,而且企业内部网络还需要提供可以从 Internet 进行访问的 HTTP 服务来进行企业宣传,这时候就会同时用到网络地址端口转换和静态网络地址转换两种网络地址转换技术。

3.3 静态网络地址转换

静态网络地址转换是最简单的一种网络地址转换形式。在静态网络地址转换中,需要手工配置从内部本地地址到内部全局地址的一对一映射关系,配置完成后这些映射关系将一直存在,直到被手工删除。静态网络地址转换一般为需要对外部网络提供服务的内网服务器提供地址转换。

3.3.1 H3C 设备静态 NAT 配置

H3C 设备静态网络地址转换涉及的配置命令如下:

```
[H3C]nat static local-ip global-ip
[H3C]interface interface-type interface-number
[H3C-Ethernet0/0]nat outbound static
```

首先指定内部本地地址和内部全局地址之间的映射关系,然后在路由器相应的接口上应用静态网络地址转换。

假设存在如图 3-2 所示的网络,要求将内网服务器的 IP 地址静态转换到 202.207.120.100,使其可以为外部网络提供 HTTP 服务。

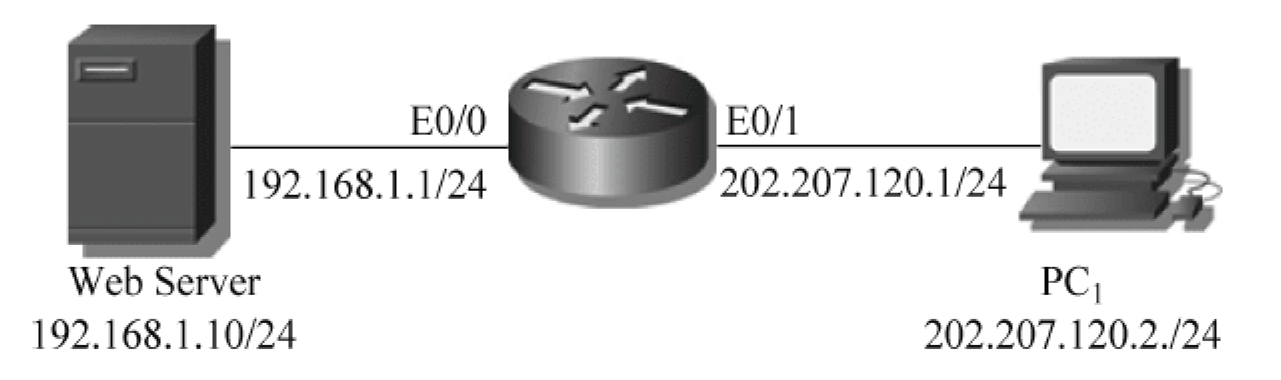


图 3-2 静态网络地址转换

具体的配置命令如下:

```
[H3C]nat static 192.168.1.10 202.207.120.100
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound static
```

配置完成后,在路由器上执行 display nat static 命令,显示结果如下:

```
[H3C]display nat static
NAT static information:
  There are currently 1 NAT static configuration(s)
  single static:
    Local-IP          : 192.168.1.10
```

```
    Global-IP          : 202.207.120.100
    Local-VPN          : ---

NAT static enabled information:
  Interface                                         Direction
  Ethernet0/1                                       out-static
```

从显示的结果可以看出，在路由器上配置了内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的静态网络地址转换，该静态地址转换应用到了接口 Ethernet0/1 的 out bound 方向上。

需要注意的是，所有的内部网络地址转换都需要应用在出站接口的 outbound 方向上。

此时，在 PC_1 上使用内部全局地址 202.207.120.100 可以访问到内网服务器的 Web 服务。进行 Web 访问的同时在路由器的用户视图下可以使用 debugging nat packet 命令查看网络地址转换的过程，显示结果如下：

```
<H3C>terminal monitor
<H3C>terminal debugging
<H3C>debugging nat packet
Info: NAT packet debugging is enabled!
<H3C>
 * Nov 15 07:26:47:904 2011 H3C NAT/7/debug:
(Ethernet0/1-in:)Pro : TCP
(202.207.120.2: 4981 - 202.207.120.100: 80) ------>
(202.207.120.2: 4981 -192.168.1.10: 80)
 * Nov 15 07:26:47:906 2011 H3C NAT/7/debug:
(Ethernet0/1-out:)Pro : TCP
(192.168.1.10: 80-202.207.120.2: 4981) ------>
(202.207.120.100: 80 -202.207.120.2: 4981)
```

从显示的结果可以看出，在 PC_1 访问 Web 服务器的数据报文进入路由器接口 Ethernet0/1 时，会将数据报文的目的 IP 地址 202.207.120.100 转换为内部本地地址 192.168.1.10；而在 Web 服务器返回给 PC_1 的数据报文从路由器的接口 Ethernet0/1 出站之前，会将数据报文的源 IP 地址 192.168.1.10 转换为内部全局地址 202.207.120.100。

需要注意的是，在 H3C 的设备上所有的 debug 类的命令都只能在用户视图下执行，而且在使用 debug 类命令进行系统调试之前，需要先执行 terminal monitor 和 terminal debugging 命令。其中，terminal monitor 命令用来开启控制台对系统信息的监视功能（该功能默认开启，因此可以不执行这条命令）；terminal debugging 命令用来开启调试信息的屏幕输出开关，使调试信息可以在终端上进行显示。

在 PC_1 上访问 Web 服务器后，在路由器上执行 display nat session 命令，显示结果如下：

```
[H3C]display nat session
There are currently 1 NAT session:
Protocol     GlobalAddr       Port      InsideAddr     Port     DestAddr   Port
  ---        202.207.120.100  0         192.168.1.10   0          ---       ---
```

```
status:800       TTL:00:05:00    Left:00:04:56    VPN:---
```

从显示的结果可以看出，当前存在一个 NAT 会话，为内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的映射。

3.3.2 Cisco 设备静态 NAT 配置

Cisco 设备静态网络地址转换涉及的配置命令如下：

```
Router(config)# ip nat inside source static local-ip global-ip
Router(config)# interface interface-type interface-number
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface interface-type interface-number
Router(config-if)# ip nat outside
```

需要注意的是，H3C 设备上只需要在连接外部网络的接口上配置 nat outbound 命令来应用 NAT，与 H3C 不同，在 Cisco 设备上需要在连接内部网络的接口上配置 ip nat inside，在连接外部网络的接口上配置 ip nat outside。

在此依然使用图 3-2 所示的网络进行 Cisco 设备静态 NAT 的配置，具体的配置命令如下：

```
Router(config)# ip nat inside source static 192.168.1.10 202.207.120.100
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat outside
```

配置完成后，在路由器上执行 show ip nat translations 命令，显示结果如下：

```
Router# show ip nat translations
Pro     Inside global      Inside local       Outside local      Outside global
---     202.207.120.100    192.168.1.10       ---                ---
```

从显示的结果可以看出，在路由器上存在一条内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的静态网络地址转换。

此时，在 PC_1 上使用内部全局地址 202.207.120.100 可以访问到内网服务器的 Web 服务。进行 Web 访问的同时，在路由器的用户视图下可以使用 debug ip nat 命令查看网络地址转换的过程，显示结果如下：

```
Router# debug ip nat
IP NAT debugging is on
Router#
* Mar  1 01:48:40.963: NAT: s=202.207.120.2, d=202.207.120.100->192.168.1.10
[6358]
* Mar  1 01:48:40.967: NAT: s=192.168.1.10->202.207.120.100, d=202.207.120.2
[6609]
```

在路由器上执行 show ip nat statistics 命令查看 NAT 的统计信息，显示结果如下：

```
Router# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0
Hits: 18    Misses: 0
Expired translations: 0
Dynamic mappings:
```

注意：静态网络地址转换由于需要静态地指定从内部本地地址到内部全局地址的一对一的映射，因此无法实现 IP 地址的节约。

3.4　动态网络地址转换

动态网络地址转换又称为 Basic NAT，动态网络地址转换也是一种一对一的映射关系，但是与静态网络地址转换不同的是，动态网络地址转换的映射关系不是一直存在的，而是只有在出口路由器的出站接口上出现符合地址转换条件的内网流量时才会触发路由器进行网络地址的转换。而且映射关系不会一直存在，到达老化时间以后就会被删除，以便于将回收的内部全局地址映射给其他需要的内部本地地址。

3.4.1　H3C 设备动态 NAT 配置

H3C 设备动态网络地址转换涉及的配置命令如下：

(1) 创建一个 ACL 用于匹配需要进行动态网络地址转换的内部本地地址。

[H3C]acl number *acl-number*
[H3C-acl-basic-2000]rule [*rule-id*] {deny|permit} [source {*sour-addr sour-wildcard*|any}]

在 NAT 中使用 ACL 匹配内部本地地址时需要注意以下 3 点。

① 不必使用 firewall enable 命令启用防火墙。

② ACL 中只有被显式规则 permit 的源 IP 地址才会进行地址转换，默认允许所有的规则不生效。

③ 如果内网中有些特殊的 IP 地址不需要做动态网络地址转换，例如，内部服务器要做静态网络地址转换，则应将其在定义 ACL 时首先 deny 掉。

(2) 创建一个存放有内部全局地址的地址池。

[H3C]nat address-group *group-number start-addr end-addr*

(3) 在出口路由器的出站接口上配置 ACL 与地址池的关联。

[H3C-Ethernet0/0]nat outbound *acl-number* address-group *group-number* no-pat

注意：no-pat 参数表示是一个 Basic NAT 的转换，不做地址的过载。

假设存在如图 3-3 所示的网络，要求将内部网络 IP 地址段 192.168.1.0/24 动态转换到 202.207.120.10～202.207.120.50。

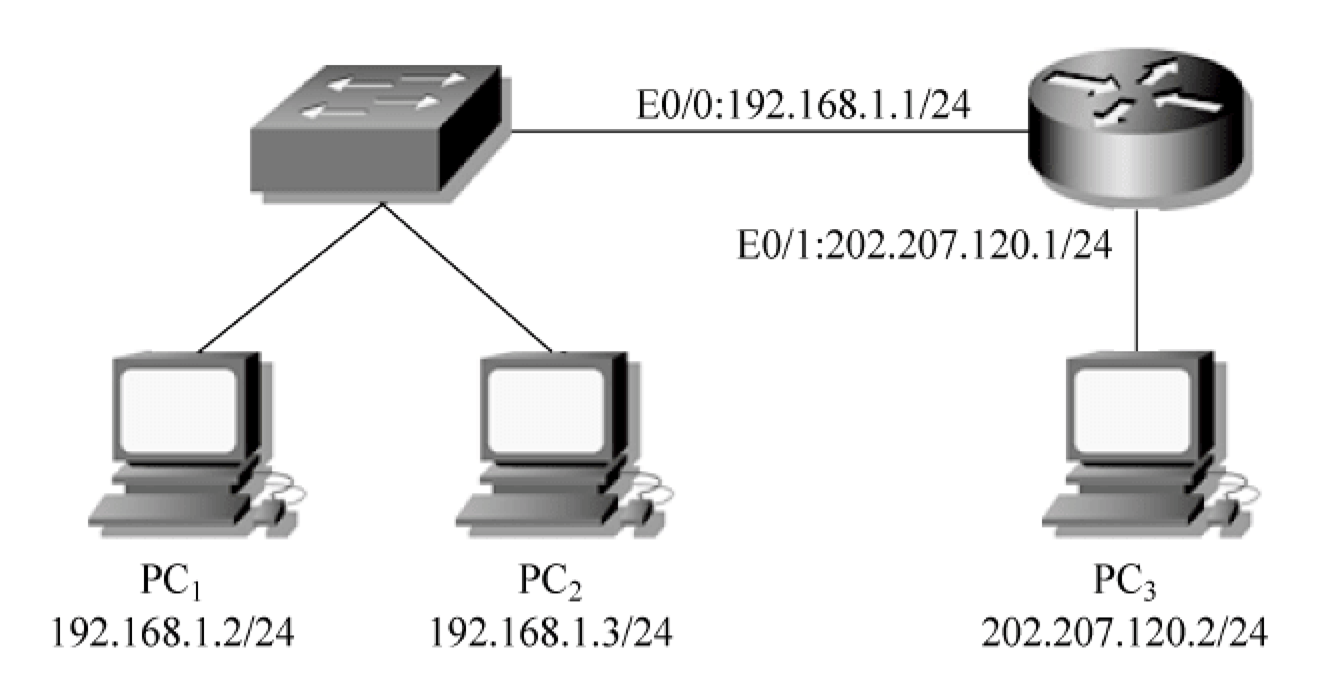


图 3-3 动态网络地址转换

具体的配置命令如下:

```
[H3C]acl number 2000
[H3C-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]nat address-group 1 202.207.120.10 202.207.120.50
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound 2000 address-group 1 no-pat
```

配置完成后,从 PC_1 去 ping PC_3,同时在路由器上执行 debugging nat packet 命令,显示结果如下:

```
<H3C>debugging nat packet
Info: NAT packet debugging is enabled!
<H3C>
*Nov 15 08:48:17:170 2011 H3C NAT/7/debug:
(Ethernet0/1-out :)Pro : ICMP
(192.168.1.2: 512 -202.207.120.2:512) ------>
(202.207.120.10: 512 -202.207.120.2:512)
*Nov 15 08:48:17:171 2011 H3C NAT/7/debug:
(Ethernet0/1-in:)Pro : ICMP
(202.207.120.2:512 -202.207.120.10:512) ------>
(202.207.120.2:512 -192.168.1.2:512)
```

从显示的结果可以看出数据报文在路由器上进行双向地址转换的过程。

在路由器上执行 display nat session 命令,显示结果如下:

```
[H3C]display nat session
There are currently 2 NAT sessions:
Protocol     GlobalAddr        Port    InsideAddr     Port      DestAddr      Port
  ---          202.207.120.10    ---     192.168.1.2    ---         ---          ---
      status:NOPAT    TTL:00:04:00    Left:00:03:54    VPN:---

     ICMP   202.207.120.10    512     192.168.1.2     512     202.207.120.2   512
      status:NOPAT    TTL:00:00:10    Left:00:00:04    VPN:---
```

从显示的结果可以看出,当前存在两个 NAT 会话,其中一个是内部本地地址

192.168.1.2到内部全局地址 202.207.120.10 的映射，生存时间为 4min；另一个为基于 ICMP 协议的映射关系，是内部本地地址 192.168.1.2 和端口号 512 到内部全局地址 202.207.120.10 和端口号 512 的映射，生存时间为 10s。在从 PC_1 去 ping PC_3 时，这两条会话会同时出现。关于不同协议的 NAT 会话生存时间可以通过 display nat aging-time 命令来查看。

其实在看到上面 display nat session 显示的结果时，还会有一个疑问：ICMP 协议处于网络层，ICMP 协议的数据报文根本不会有传输层的封装，因此也就不可能会有端口号的存在，那端口号 512 又是从哪里来的呢？实际上 512 并不是端口号，而是 ICMP 报头封装中的 Identifier 字段（即标识字段）的值。在定义 ICMP 协议的请求注解文档 RFC792 中，描述 Identifier 字段可以像 TCP 或 UDP 协议的端口号一样来区分不同的 ICMP 进程，但实际上在特定的操作系统中，ICMP 协议的 Identifier 字段是一个定值。例如，在 Windows XP 系统中，ICMP 协议封装中的 Identifier 字段的值为 0x0200，即十进制的 512，这一点可以在 Wireshark 软件捕获的 ICMP 请求/应答报文的报头中看到。因此 Identifier 字段实际上并不具备区分进程的功能，ICMP 进程的区分实际上使用的是 Sequence number 字段。而 Identifier 字段的一个重要功能就是在 NAT 中作为地址映射的依据，因此在 display nat session 命令的显示结果中会看到 ICMP 协议的端口号为 512。Identifier 字段会在 NAT 对 ICMP 分片报文的处理中发挥非常重要的作用，在此不再进行介绍，感兴趣的学生可以自行查阅相关资料。

在进行动态网络地址转换时，路由器总是会从地址池中拿第一个可用地址来进行映射，此时如果 PC_2 去 ping PC_3，则会为 PC_2 分配内部全局地址 202.207.120.11。

可以在用户视图下使用 reset nat session 命令清除掉未到老化时间的地址映射关系。

3.4.2　Cisco 设备动态 NAT 配置

在 Cisco 设备上动态 NAT 的配置同样需要创建匹配内部本地地址的 ACL 和存放内部全局地址的地址池，涉及的命令如下：

```
Router(config)#access-list access-list-number {permit|deny} source [source-wildcard]
Router(config)#ip nat pool pool-name start-addr end-addr netmask netmask
Router(config)#ip nat inside source list access-list-number pool pool-name
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat outside
```

在此依然使用图 3-3 所示的网络进行 Cisco 设备动态 NAT 的配置，具体的配置命令如下：

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool dyn-nat 202.207.120.10 202.207.120.50 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool dyn-nat
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat inside
```

```
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
```

配置完成后,从 PC_1 去 ping PC_3,同时在路由器上执行 debugging nat packet 命令,显示结果如下:

```
Router#debug ip nat
IP NAT debugging is on
Router#
*Mar  1 00:08:43.359: NAT: s=192.168.1.2->202.207.120.10, d=202.207.120.2 [7745]
*Mar  1 00:08:43.359: NAT*: s=202.207.120.2, d=202.207.120.10->192.168.1.2 [7037]
```

在路由器上执行 show ip nat translations 命令,显示结果如下:

```
Router#show ip nat translations
Pro   Inside global      Inside local     Outside local     Outside global
---   202.207.120.10     192.168.1.2      ---               ---
```

3.5 网络地址端口转换

网络地址端口转换(Network Address Port Translation,NAPT)又称为端口地址转换(Port Address Translation,PAT)或者地址过载。动态网络地址转换是一对一的映射关系,它只是解决了内外网通信的问题,但并没有真正意义上解决公有 IP 地址不足的问题。而 NAPT 技术通过使用同一个内部全局地址的不同端口号来标识不同的内部本地地址,实现多对一的地址转换,从而实现公有 IP 地址的节约。

在 NAPT 的转换过程中,路由器维护着如表 3-3 所示的动态地址转换表,通过端口的映射关系使多个内部本地地址转换到一个内部全局地址上。在进行地址转换时,一般会尽量使用与本地地址端口相同的全局地址端口,但如果该端口已经被使用,则会选择最小的可用端口作为全局地址端口。

表 3-3 NAPT 地址转换表

内部本地地址	内部本地地址端口	内部全局地址	内部全局地址端口
192.168.1.2	2000	202.207.120.10	2000
192.168.1.3	1024		1024
192.168.1.20	1024		1025

3.5.1 H3C 设备 NAPT 配置

在 H3C 设备上 NAPT 的配置方法与 Basic NAT 基本相同,唯一的区别是 NAPT 在出口路由器的出站接口上配置 ACL 与地址池的关联时不使用 no-pat 参数,表明是基于端口的多对一的地址转换。

在此依然使用图 3-3 所示的网络,要求将内部网络 192.168.1.0/24 使用 NAPT 技术过载到唯一的内部全局地址 202.207.120.10 上。具体的配置命令如下:

```
[H3C]acl number 2000
[H3C-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]nat address-group 1 202.207.120.10 202.207.120.10
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound 2000 address-group 1
```

配置完成后，在 PC_1 和 PC_2 上分别去 ping PC_3，然后在路由器上执行 display nat session 命令，显示结果如下：

```
[H3C]display nat session
There are currently 2 NAT sessions:
Protocol   GlobalAddr       Port     InsideAddr    Port      DestAddr        Port
ICMP       202.207.120.10   12288    192.168.1.2   512       202.207.120.2   512
      status:11       TTL:00:00:10   Left:00:00:04   VPN:---
ICMP       202.207.120.10   12289    192.168.1.3   512       202.207.120.2   512
      status:11       TTL:00:00:10   Left:00:00:06   VPN:---
```

从显示的结果可以看出，内部本地地址 192.168.1.2 和 192.168.1.3 均转换到了内部全局地址 202.207.120.10，分别用端口号 12288 和 12289 来区分。

3.5.2　Cisco 设备 NAPT 配置

在 Cisco 设备上 NAPT 的配置方法和动态 NAT 基本相同，唯一的区别是配置 NAPT 时在进行 ACL 和地址池关联的指令中增加了一个 overload 参数，用来表明是基于端口的多对一的地址转换。

在此依然使用图 3-3 所示的网络，要求将内部网络 192.168.1.0/24 使用 NAPT 技术过载到唯一的内部全局地址 202.207.120.10 上。具体的配置命令如下：

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool napt 202.207.120.10 202.207.120.10 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool napt overload
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
```

配置完成后，在 PC_1 和 PC_2 上分别去 ping PC_3，然后在路由器上执行 display nat session 命令，显示结果如下：

```
Router#show ip nat translations
Pro    Inside global        Inside local       Outside local       Outside global
icmp   202.207.120.10:512   192.168.1.2:512    202.207.120.2:512   202.207.120.2:512
icmp   202.207.120.10:513   192.168.1.3:512    202.207.120.2:512   202.207.120.2:513
```

从显示的结果可以看出，内部本地地址 192.168.1.2 和 192.168.1.3 均转换到了内部全局地址 202.207.120.10，分别用端口号 512 和 513 来区分。

3.6 基于接口的地址转换

基于接口的地址转换又称为 Easy IP,是 NAPT 的一种特殊形式。在 NAPT 技术中,由于需要配置存放有内部全局地址的地址池,因此需要预先确定可以使用的公有 IP 地址范围,但是在目前应用非常广泛的 ADSL 接入中,公有 IP 地址是由服务提供商动态分配的,无法提前预知,而且服务提供商只会为用户分配一个公有 IP。在这种情况下,就需要使用 Easy IP 技术来实现地址转换。Easy IP 与 NAPT 的区别在于它是将内部本地地址全部映射到出口路由器的出站接口地址上。除了 ADSL 外,一般在计算机机房和网吧中也都采用 Easy IP 技术来进行地址的转换,以实现 IP 地址的节约。

3.6.1 H3C 设备 Easy IP 配置

由于内部全局地址使用路由器的接口地址,因此在 Easy IP 的配置中,不需要定义地址池,其他配置与 NAPT 类似。

在此依然使用图 3-3 所示的网络,要求将内部网络 192.168.1.0/24 使用 Easy IP 技术进行地址转换,具体的配置命令如下:

```
[H3C]acl number 2000
[H3C-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound 2000
```

配置完成后,在 PC_1 和 PC_2 上分别去 ping PC_3,然后在路由器上执行 display nat session 命令,显示结果如下:

```
[H3C]display nat session
There are currently 2 NAT sessions:
Protocol    GlobalAddr     Port     InsideAddr    Port    DestAddr       Port
ICMP        202.207.120.1  12288    192.168.1.2   512     202.207.120.2  512
    status:11      TTL:00:00:10    Left:00:00:05     VPN:---

ICMP        202.207.120.1  12289    192.168.1.3   512     202.207.120.2  512
    status:11      TTL:00:00:10    Left:00:00:06     VPN:---
```

从显示的结果可以看出,内部本地地址 192.168.1.2 和 192.168.1.3 均转换到了路由器接口 Ethernet0/1 的 IP 地址 202.207.120.1 上。

3.6.2 Cisco 设备 Easy IP 配置

在 Cisco 设备上 Easy IP 的配置涉及的命令如下:

Router(config)#access-list *access-list-number* {permit|deny} *source* [*source-wildcard*]
Router(config)#ip nat inside source list *access-list-number* interface *interface-type interface-number* overload
Router(config)#interface *interface-type interface-number*
Router(config-if)#ip nat inside

```
Router(config-if)# exit
Router(config)# interface interface-type interface-number
Router(config-if)# ip nat outside
```

在此依然使用图 3-3 所示的网络，要求将内部网络 192.168.1.0/24 使用 Easy IP 技术进行地址转换，具体的配置命令如下：

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface FastEthernet 0/1 overload
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip nat outside
```

配置完成后，在 PC_1 和 PC_2 上分别去 ping PC_3，然后在路由器上执行 show ip nat translations 命令，显示结果如下：

```
Router# show ip nat translations
Pro    Inside global        Inside local       Outside local        Outside global
icmp   202.207.120.1:512    192.168.1.2:512    202.207.120.2:512    202.207.120.2:512
icmp   202.207.120.1:513    192.168.1.3:512    202.207.120.2:512    202.207.120.2:513
```

从显示的结果可以看出，内部本地地址 192.168.1.2 和 192.168.1.3 均转换到了路由器接口 FastEthernet 0/1 的 IP 地址 202.207.120.1 上。

3.7　端口地址重定向

无论是 Basic NAT，还是 NAPT 和 Easy IP，都是动态的地址转换，映射关系是由内网主机向外网发出的访问触发建立的，而外网主机无法主动连接内网主机。对于内网存在服务器的情况，只能采用静态网络地址转换。但是在有些情况下，公有 IP 地址很少，不足以满足内网服务器的静态转换需求。例如，只有一个公有 IP 地址被分配给出口路由器的出站接口，内网的主机通过 Easy IP 实现地址转换，如果内网存在服务器的情况下，显然无法使用静态网络地址转换，这时候就可以使用端口地址重定向技术来实现。

端口地址重定向又称为 NAT Server。它通过将“内部本地地址＋端口”静态地映射到“内部全局地址＋端口”，从而确保外网主机可以主动访问内网服务器某些服务的同时不增加公有 IP 地址。

3.7.1　H3C 设备 NAT Server 配置

H3C 设备端口地址重定向需要在接口视图下进行配置，具体的配置命令如下：

```
[H3C-Ethernet0/0]nat server protocol pro-type global global-addr [global-port] inside host-addr
[host-port]
```

在 3.6 节的基础上，进行端口地址重定向的配置，要求将内网 Web 服务器 192.168.1.2 通过 NAT Server 静态映射到出口路由器出站接口的 80 端口上，使外部网络主机 PC_3 可

以访问 PC_1 的 Web 服务,具体的配置命令如下:

```
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat server protocol tcp global 202.207.120.1 80 inside 192.168.1.2 80
```

配置完成后,在路由器上执行 display nat server 命令,显示结果如下:

```
[H3C]display nat server
NAT server in private network information:
  There are currently 1 internal server(s)
  Interface: Ethernet0/1, Protocol: 6(tcp)
  Global: 202.207.120.1 : 80(www)
  Local : 192.168.1.2 : 80(www)
```

从显示的结果可以看出,在路由器的接口 Ethernet0/1 上配置了一个基于 TCP 协议的 NAT Server,其映射关系为"内部本地地址 192.168.1.2+端口号 80"映射到"内部全局地址 202.207.120.1+端口号 80"。

此时在 PC_3 的 IE 浏览器中输入 202.207.120.1,应该可以访问 PC_1 上的 Web 服务。同时在路由器上执行 debugging nat packet 命令,显示结果如下:

```
<H3C>debugging nat packet
Info: NAT packet debugging is enabled!
<H3C>
*Nov 16 03:29:58:867 2011 H3C NAT/7/debug:
(Ethernet0/1-in:)Pro : TCP   is to NAT server
(202.207.120.2: 2196 -202.207.120.1: 80) ------>
(202.207.120.2: 2196 -192.168.1.2: 80)
*Nov 16 03:29:58:868 2011 H3C NAT/7/debug:
(Ethernet0/1-out:)Pro: TCP   is from NAT server
(192.168.1.2: 80 -202.207.120.2: 2196) ------>
(202.207.120.1: 80 -202.207.120.2: 2196)
```

从显示的结果可以看出,通过 NAT Server 技术实现了"202.207.120.1+80"和"192.168.1.2+80"之间的转换。

3.7.2 Cisco 设备 NAT Server 配置

Cisco 设备上 NAT Server 配置涉及的命令如下:

```
Router(config)#ip nat inside source static {tcp|udp} local-ip local-port global-ip global-port
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat outside
```

在 3.6 节的基础上,进行端口地址重定向的配置,要求将内网 Web 服务器 192.168.1.2 通过 NAT Server 静态映射到出口路由器出站接口的 80 端口上,使外部网络主机 PC_3 可以访问 PC_1 的 Web 服务,具体的配置命令如下:

```
Router(config)#ip nat inside source static tcp 192.168.1.2 80 202.207.120.1 80
```

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
```

配置完成后，在路由器上执行 show ip nat translations 命令，显示结果如下：

```
Router#show ip nat translations
Pro    Inside global      Inside local      Outside local      Outside global
tcp    202.207.120.1:80   192.168.1.2:80    ---                ---
```

此时在 PC_3 的 IE 浏览器中输入 202.207.120.1 可以访问 PC_1 上的 Web 服务。同时在路由器上执行 debug ip nat 命令，显示结果如下：

```
Router#debug ip nat
IP NAT debugging is on
Router#
*Mar  1 00:28:43.615: NAT: s=202.207.120.2, d=202.207.120.1->192.168.1.2 [9331]
*Mar  1 00:28:43.619: NAT: s=192.168.1.2->202.207.120.1, d=202.207.120.2 [10216]
```

3.8 NAT 与 ACL 的顺序关系

通过对前几节内容的学习，已经知道 NAT 一般需要应用在出口路由器的出站接口上，而在该接口上往往也会应用 ACL 来保护内部网络的安全，在这种情况下就会涉及 ACL 和 NAT 处理的先后顺序问题，处理顺序的不同会影响到对 ACL 具体规则的定义。不同厂家的网络设备在处理顺序上会有所不同，在这里可以通过实验来验证 H3C 路由器对 ACL 和 NAT 的处理顺序。

在此依然使用图 3-3 所示的网络，为了验证简单起见，将内部网络主机 PC_1 和 PC_2 的 IP 地址分别静态转换到内部全局地址 202.207.120.20 和 202.207.120.30 上。具体的配置命令如下：

```
[H3C]nat static 192.168.1.2 202.207.120.20
[H3C]nat static 192.168.1.3 202.207.120.30
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound static
```

配置完成后，在 PC_1 或 PC_2 上可以 ping 通 PC_3，并且在路由器上使用 display nat session 命令可以看到内部本地地址 192.168.1.2 到内部全局地址 202.207.120.20、内部本地地址 192.168.1.3 到内部全局地址 202.207.120.30 之间的映射关系。

配置基本 ACL 并进行应用，具体的配置命令如下：

```
[H3C]firewall enable
[H3C]acl number 2000
[H3C-acl-basic-2000]rule deny source 192.168.1.2 0
[H3C-acl-basic-2000]rule permit
```

```
[H3C-acl-basic-2000]quit
[H3C]inter Ethernet 0/1
[H3C-Ethernet0/1]firewall packet-filter 2000 outbound
```

从上面的配置可以看出,ACL 2000中的规则rule 0的定义是拒绝源IP地址为内部本地地址192.168.1.2的数据流量,该ACL被应用在路由器的Ethernet 0/1接口的outbound方向上。

配置完成后,在PC_1上使用ping命令测试到达PC_3的联通性,会发现无法联通。在路由器上执行命令display acl 2000,显示结果如下:

```
[H3C]display acl 2000
Basic ACL  2000, named -none-, 2 rules
ACL's step is 5
rule 0 deny source 192.168.1.2 0 (4 times matched)
rule 5 permit
```

从显示的结果可以看出,PC_1发出的流量命中规则rule 0,因而被拒绝。因此通过推断可知,在路由器某个接口上同时存在出站ACL和NAT时,出站流量应该是先去匹配出站ACL,然后再进行地址的转换,具体如图3-4所示。

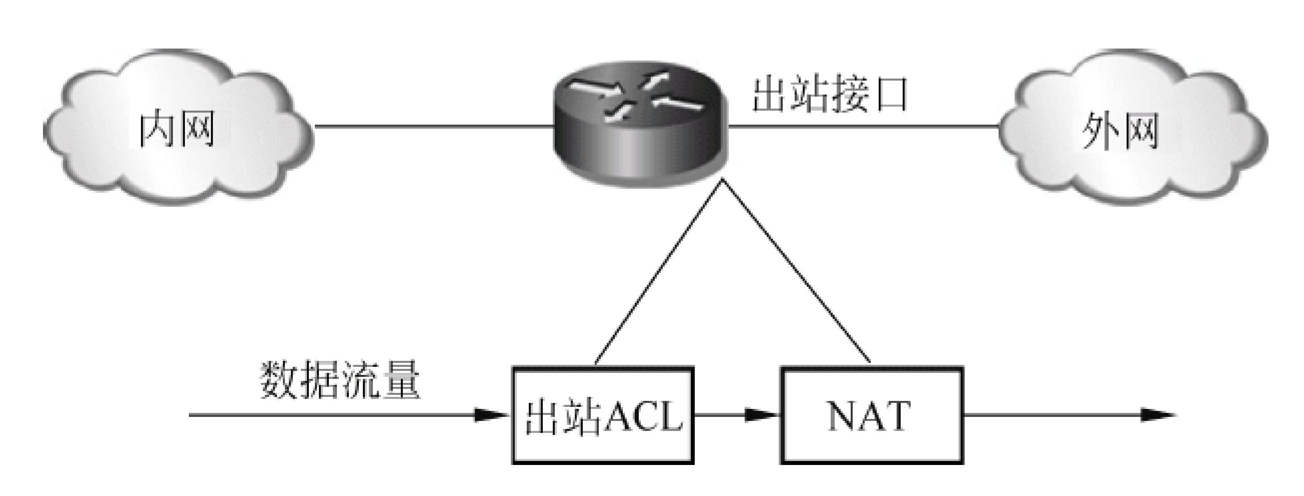


图3-4 出站ACL与NAT的顺序关系

将ACL 2000修改如下:

```
[H3C]acl number 2000
[H3C-acl-basic-2000]undo rule 0
[H3C-acl-basic-2000]rule 0 deny source 202.207.120.20 0
```

修改完成后,在PC_1上再次使用ping命令测试到达PC_3的联通性,会发现此时可以联通,从而进一步验证了图3-4所示的顺序关系。

实际上在出口路由器的出站接口上很少使用出站ACL,而更多的时候是使用入站ACL来对外部网络需要进入内部网络的流量进行访问控制。为验证入站ACL和NAT的处理顺序,在路由器上配置高级ACL并进行应用,具体的配置命令如下:

```
[H3C]acl number 3000
[H3C-acl-adv-3000]rule deny ip destination 192.168.1.2 0
[H3C-acl-adv-3000]rule permit ip
[H3C-acl-adv-3000]quit
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]undo firewall packet-filter 2000 outbound
[H3C-Ethernet0/1]firewall packet-filter 3000 inbound
```

从上面的配置可以看出，ACL 3000 中的规则 rule 0 的定义是拒绝目的 IP 地址为内部本地地址 192.168.1.2 的数据流量，该 ACL 被应用在路由器 Ethernet 0/1 接口的 inbound 方向上。

注意：为保证测试的简单和纯粹，在应用 ACL 3000 之前，建议将 ACL 2000 的应用从接口 Ethernet 0/1 上去掉。

配置完成后，在 PC_3 上使用命令 ping 202.207.120.20 测试到达 PC_1 的联通性，会发现无法联通。在路由器上执行命令 display acl 3000，显示结果如下：

```
[H3C]display acl 3000
Advanced ACL  3000, named -none-, 2 rules
ACL's step is 5
rule 0 deny ip destination 192.168.1.2 0 (4 times matched)
rule 5 permit ip
```

从显示的结果可以看出，PC_3 发出的流量命中规则 rule 0，因而被拒绝。因此通过推断可知，在路由器某个接口上同时存在入站 ACL 和 NAT 时，入站流量应该是先进行地址的转换，然后去匹配入站 ACL。具体如图 3-5 所示。

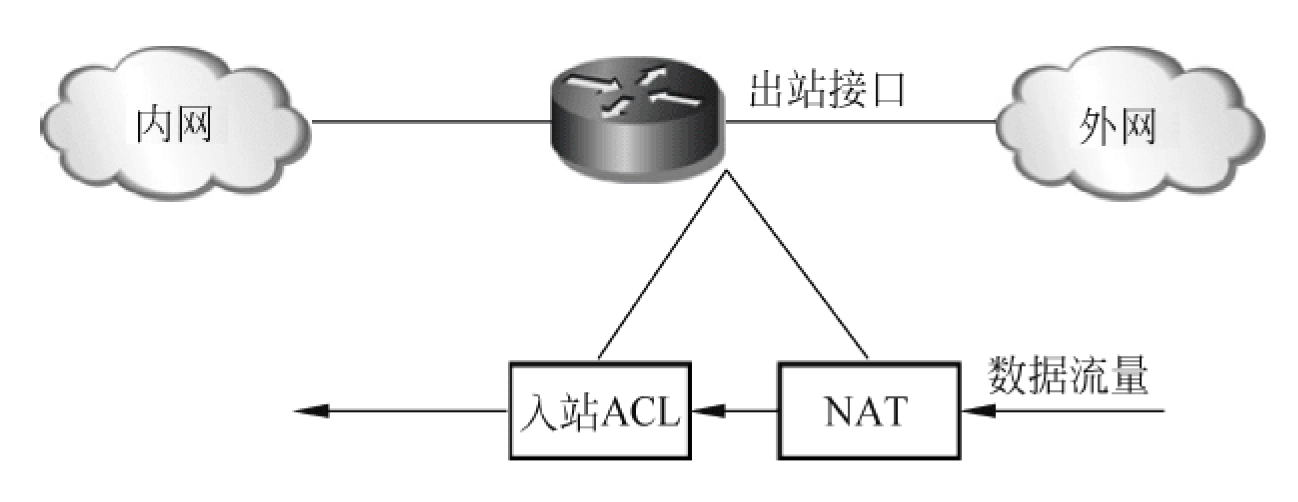


图 3-5　入站 ACL 与 NAT 的顺序关系

将 ACL 3000 修改如下：

```
[H3C]acl number 3000
[H3C-acl-adv-3000]undo rule 0
[H3C-acl-adv-3000]rule 0 deny ip destination 202.207.120.20 0
```

修改完成后，在 PC_3 上再次使用命令 ping 202.207.120.20 测试到达 PC_1 的联通性，会发现此时可以联通，从而进一步验证了图 3-5 所示的顺序关系。

注意：Cisco 路由器在对 ACL 和 NAT 的处理顺序上与 H3C 路由器正好相反，因此在定义 ACL 规则时一定要注意根据网络设备对 ACL 和 NAT 的处理顺序来决定是对内部本地地址进行约束，还是对内部全局地址进行约束。对于 H3C 的路由器而言，ACL 的定义总是约束内部本地地址；而对于 Cisco 的路由器而言，ACL 的定义则总是约束内部全局地址。

3.9　NAT ALG 技术

传统的 NAT 技术只能识别 IP 报头中的 IP 地址以及传输层报头中的端口号并对其进行转换，但无法对应用层数据信息进行识别。然而在实际的应用中，很多应用层协议的报文中可能会携带 IP 地址和端口号信息。例如，典型的多通道应用层协议 FTP 需要在控制通

道上对后续的数据通道的 IP 地址和端口号进行协商；DNS 响应报文中包含为相关域名解析出的 IP 地址；网络层协议 ICMP 的差错报文中也包含 IP 地址。由于无法对上层协议数据载荷中的 IP 地址和端口号进行识别和转换，因此传统的 NAT 技术往往会导致部分应用无法正常使用。而通过结合应用层网关(Application Level Gateway，ALG)技术，NAT 就可以对应用层等上层数据信息进行解析，并对数据载荷内的 IP 地址和端口号等进行转换，从而保障上层应用的正确性。下面就 FTP 协议来介绍 NAT ALG 的具体应用。

Cisco 和 H3C 在 NAT ALG 的实现上完全相同，在此以 H3C 设备为例对 NAT ALG 在 FTP 中的应用进行介绍。依然使用图 3-3 所示的网络，将内部网络 192.168.1.0/24 使用 Easy IP 技术进行地址转换。具体的配置命令如下：

```
[H3C]acl number 2000
[H3C-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound 2000
```

配置完成后，在 PC_3 上启用 FTP 服务，然后在 PC_1 上使用主动模式访问 PC_3 的 FTP 服务，并分别在 PC_1 和 PC_3 上使用 Wireshark 软件捕获 FTP 数据报文，具体如图 3-6 和图 3-7 所示。

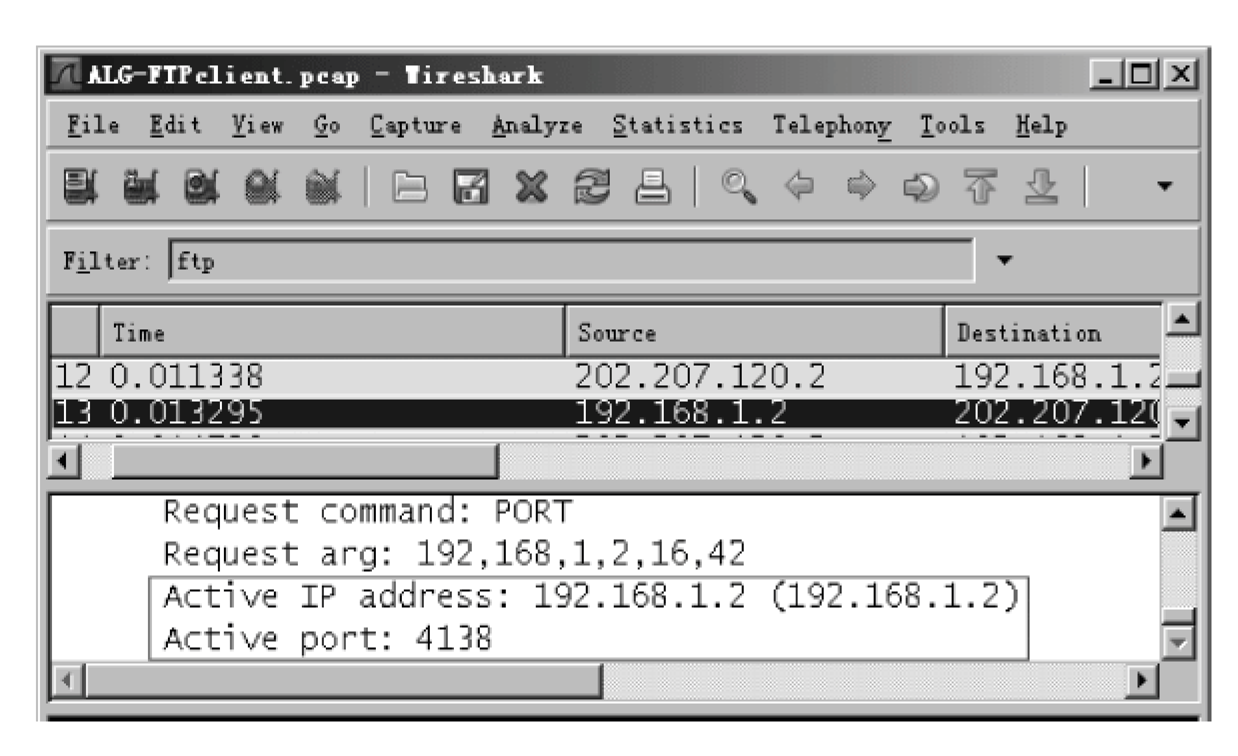


图 3-6　PC_1 上的 FTP 报文

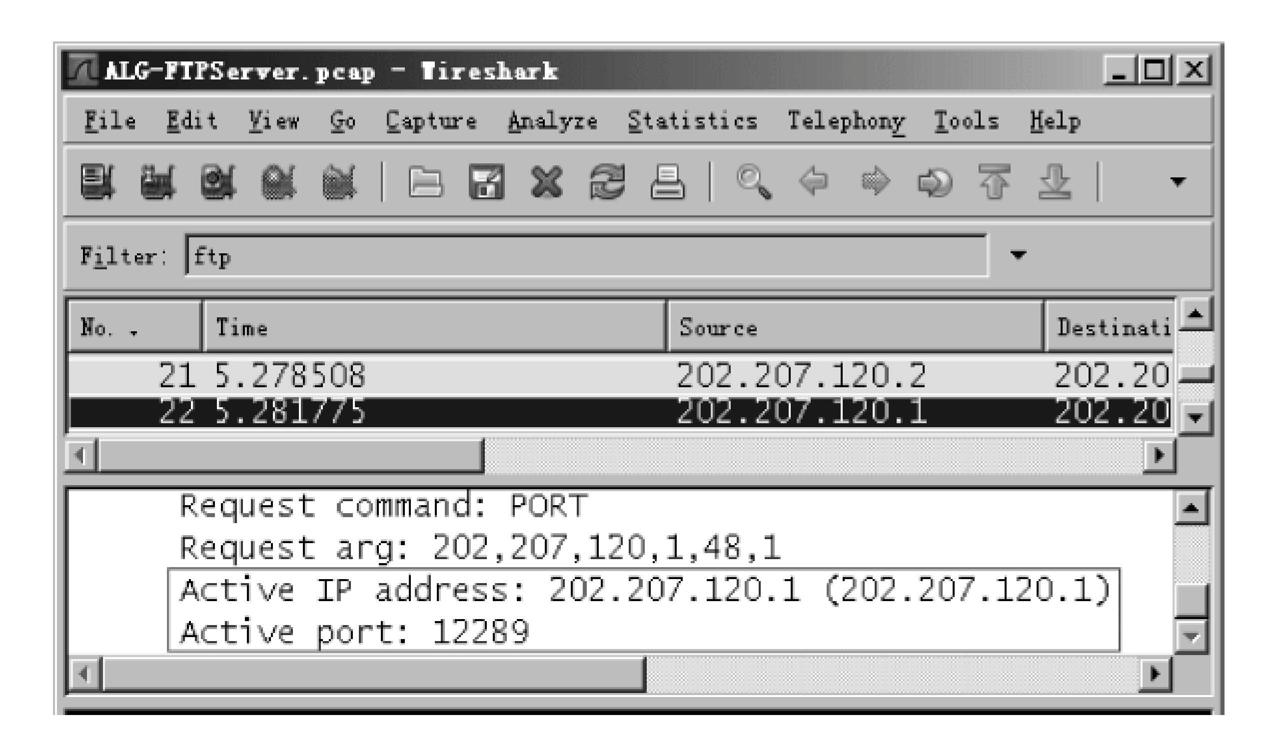


图 3-7　PC_3 上的 FTP 报文

从图 3-6 中显示的结果可以看出，由 PC_1 发出的进行数据通道协商的 PORT 报文中，Active IP address 为 192.168.1.2，Active port 为 4138，即由 PC_1 告诉 FTP 服务器 PC_3 自己将在 IP 地址 192.168.1.2 和端口 4138 上进行监听，等待 FTP 服务器发起数据连接。

从图 3-7 显示的结果可以看出，在 FTP 服务器 PC_3 接收到的 PORT 报文中，Active IP address 已经变成了 202.207.120.1，Active port 已经变成了 12289，因此 PC_3 会向 IP 地址 202.207.120.1 的 12289 端口发起数据连接。

在路由器上执行 display nat session 命令，显示结果如下：

```
[H3C]display nat session
There are currently 2 NAT sessions:
    Protocol    GlobalAddr       Port     InsideAddr     Port    DestAddr        Port
    TCP         202.207.120.1    12288    192.168.1.2    4137    202.207.120.2   21
    status:10      TTL:00:05:00    Left:00:04:23    VPN:---

    TCP         202.207.120.1    12289    192.168.1.2    4138    202.207.120.2   20
    status:251     TTL:00:05:00    Left:00:04:23    VPN:---
```

从显示的结果可以看出，对于 FTP 数据连接存在一个 NAT 会话，为“192.168.1.2＋4138”到“202.207.120.1＋12289”的映射，该映射是通过 NAT ALG 技术实现的。

结合上面的例子，可知 NAT ALG 对 FTP 报文载荷的处理流程如图 3-8 所示。

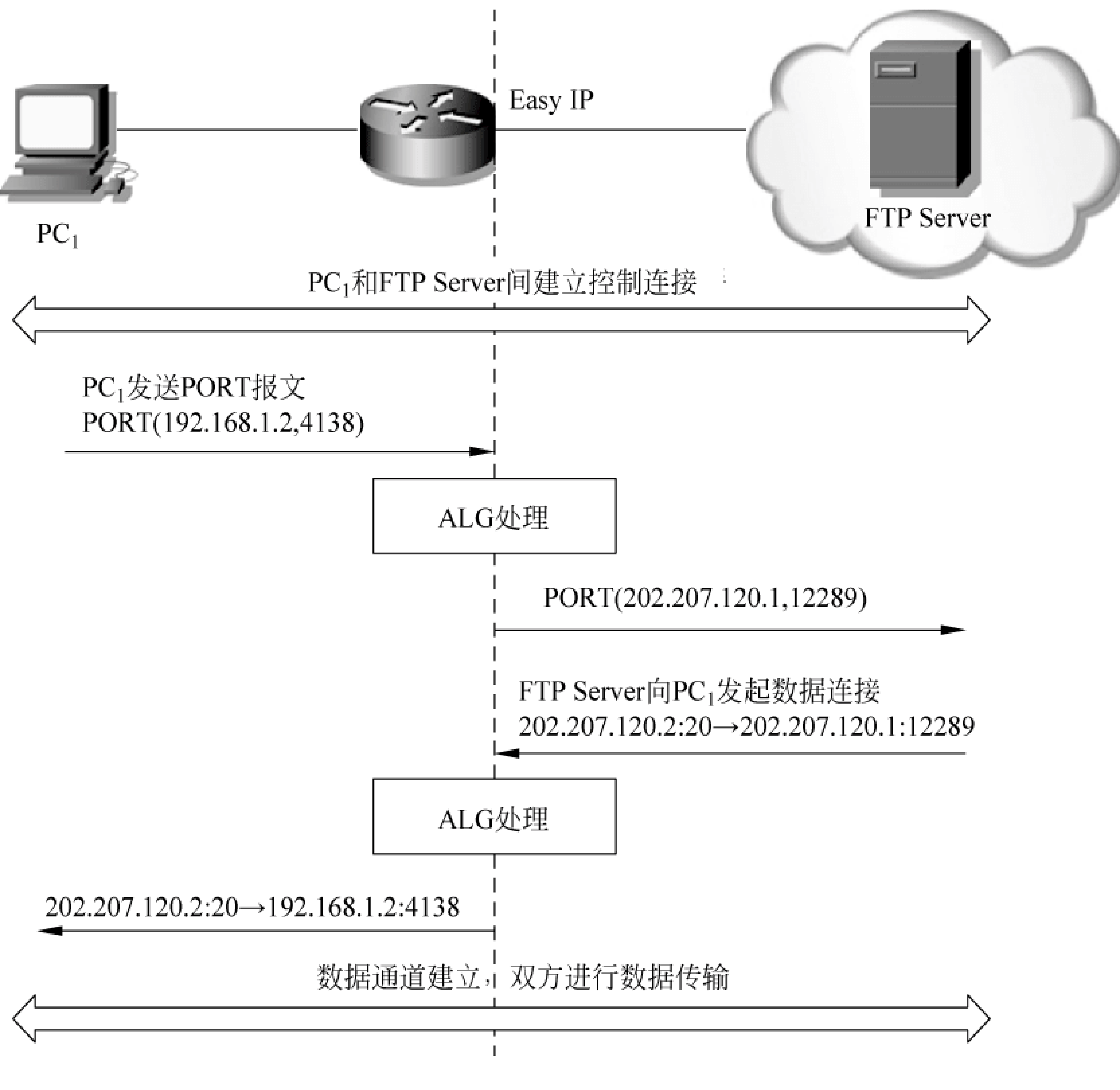


图 3-8　NAT ALG 对 FTP 报文载荷的处理流程

在路由器上,默认 NAT ALG 功能处于开启状态;如果处于关闭状态,可以通过 nat alg {all|dns|ftp|h323|ils|nbt|pptp|sip}命令开启对特定协议的 NAT ALG 的功能。不同型号的设备对于协议种类的支持可能会有所区别,要以设备的实际情况为准。

3.10　模拟公司分支机构地址转换配置方案

分支机构 B-1 需要在网络边界上使用路由器完成地址转换任务。可按表 3-4 所示地址转换方案配置边界路由器,以满足 3.1 节定义的网络地址转换任务需求。

表 3-4　分支机构网络地址转换情况

<table>
<tr><th>内网主机</th><th>地址转换类型</th><th>内部本地地址</th><th>端口</th><th>全局地址</th><th>全局地址前缀</th><th>全局端口</th><th>外部本地地址</th></tr>
<tr><td>模拟生产系统</td><td>内部静态 NAT</td><td>200.100.11.0/28</td><td>—</td><td>200.100.15.0～200.100.15.15</td><td>26</td><td>—</td><td>—</td></tr>
<tr><td>总部生产系统</td><td>外部静态 NAT</td><td>—</td><td>—</td><td>200.100.11.0～200.100.11.255</td><td>24</td><td>—</td><td>10.0.1.0/24</td></tr>
<tr><td>Ser1</td><td>内部静态 NAT</td><td>10.0.0.17/28</td><td>—</td><td>200.100.15.17</td><td>26</td><td>—</td><td>—</td></tr>
<tr><td>WebSer1</td><td>内部端口重定向</td><td>10.0.0.18/28</td><td>80</td><td rowspan="7">200.100.15.18</td><td>26</td><td>—</td><td>—</td></tr>
<tr><td rowspan="6">MailSer1</td><td rowspan="3">内部端口重定向</td><td rowspan="6">10.0.0.19/28</td><td rowspan="3">25</td><td rowspan="6">26</td><td rowspan="2">80</td><td rowspan="2">—</td></tr>
<tr></tr>
<tr><td rowspan="2">25</td><td rowspan="2">—</td></tr>
<tr><td rowspan="3">内部端口重定向</td><td rowspan="3">110</td></tr>
<tr><td rowspan="2">110</td><td rowspan="2">—</td></tr>
<tr></tr>
<tr><td>普通主机</td><td>内部动态 PAT</td><td>10.0.2.0/24</td><td>…</td><td>200.100.15.32～200.100.15.47</td><td>26</td><td>…</td><td>—</td></tr>
<tr><td>主管用机</td><td>内部动态 NAT</td><td>10.0.3.0/24</td><td>—</td><td>200.100.15.48～200.100.15.56</td><td>26</td><td>—</td><td>—</td></tr>
</table>

(1) 分支机构的模拟生产系统中各主机需要配置静态 NAT 转换,这样总部可以访问这些主机。

(2) 总部生产系统地址与模拟生产系统地址重叠,使用外部静态 NAT,将其转换为本地 10.0.3.0/24。

(3) 服务器 Ser1 上宿主多种服务,为保证网络服务性能,使用内部静态 NAT 实现对外服务。

(4) 服务器 WebSer1、MailSer1 分别提供 Web 服务和邮件服务,其服务端口不冲突,本着节省 IP 地址资源的原则,可以将其转换为一个公共 IP。

(5) 内网有 200 台左右普通主机,根据平时历史统计,每台主机对外并发连接平均在 1000 个左右,考虑到一个公共地址可以提供 4000 个左右 PAT,则至少需要 5 个公共 IP 地址,方案设计为其预留 16 个 IP 地址。

(6) 主管用机因为要访问网络多媒体资源,所以不能使用 PAT,考虑使用内部动态 NAT。

3.11　小结

作为一种缓解 IP 地址空间紧张的技术，NAT 技术被广泛应用在计算机房、网吧以及中小企业的网络中。基于模拟公司分支机构对地址转换的需求，本章对常用的几种内部网络地址转换方式，包括静态 NAT、动态 NAT、NAPT、Easy IP 以及端口地址重定向的转换原理以及配置方法进行了介绍，并简单介绍了 NAT 与 ACL 的顺序关系以及 NAT ALG 技术。

3.12　习题

1. 内部网络地址转换有哪几种不同的类型？

2. 以下 NAT 技术中，可以实现多对一映射转换的是(　　)。

A. 静态 NAT　　B. 动态 NAT　　C. Easy IP　　D. NAT ALG

3. 在配置 NAT 时，(　　)用来确定哪些内部本地地址将被转换。

A. ACL　　B. 地址池　　C. 地址转换表　　D. 进行 NAT 的接口

4. 在 H3C 设备的一个接口上同时存在 ACL 和 NAT 时，ACL 应该对内部本地地址还是内部全局地址进行约束？为什么？

3.13　实训

3.13.1　静态 NAT 与 Easy IP 配置及验证实训

实验学时：4 学时。

每组实验学生人数：4 人。

1. 实验目的

(1) 掌握静态 NAT 和 Easy IP 的配置方法。

(2) 理解静态 NAT 和 Easy IP 的工作原理及转换过程。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：5 台

(2) 路由器：4 台

(3) 三层交换机：1 台

(4) 二层交换机：1 台

(5) UTP 电缆：11 条

(6) Console 电缆：5 条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 配置静态 NAT。

(2) 配置 Easy IP。

4. 实验指导

(1) 按照图3-9所示的网络拓扑结构搭建网络,完成网络连接。其中交换机SWA与路由器RTA、RTB、RTC和RTD分别使用接口E1/0/1、E1/0/2、E1/0/3和E10/4相连。

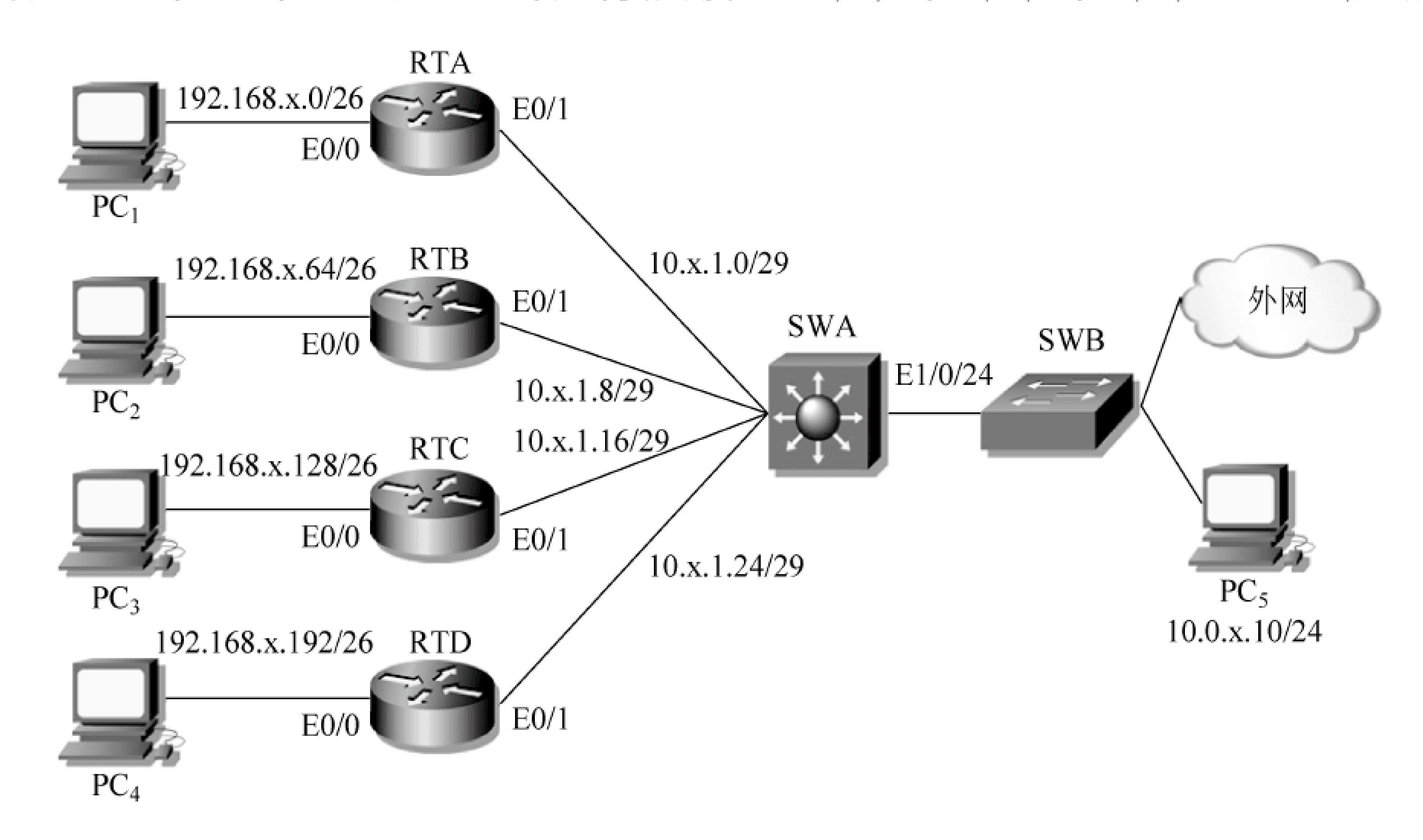


图3-9 静态NAT及Easy IP配置及验证实训

(2) 按照图3-9所示为路由器、交换机和PC配置IP地址,其中路由器的E0/0接口使用相应网段中的最后一个可用地址,PC_1~PC_4暂时使用相应网段中的第一个可用地址,路由器的E0/1接口和相连的交换机SWA的接口分别使用相应网段的前两个可用地址,PC_5的网关地址设置为交换机SWA的接口E1/0/24的IP地址10.0.x.2。在4台路由器和交换机SWA上配置默认路由保障整个网络的联通性。

H3C设备参考命令如下:

```
[RTA]interface Ethernet 0/0
[RTA-Ethernet0/0]ip address 192.168.x.62 26
[RTA-Ethernet0/0]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]ip address 10.x.1.1 29
[RTA-Ethernet0/0]quit
[RTA]ip route-static 0.0.0.0 0 10.x.1.2
--------其他3台路由器配置略--------

[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port link-mode route
[SWA-Ethernet1/0/1]ip address 10.x.1.2 29
[SWA-Ethernet1/0/1]quit
--------接口Ethernet 1/0/2、Ethernet 1/0/3、Ethernet 1/0/4配置略--------
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-mode route
[SWA-Ethernet1/0/24]ip address 10.0.x.2 24
```

```
[SWA-Ethernet1/0/24]quit
[SWA]ip route-static 0.0.0.0 0 10.0.x.1
```

Cisco 设备参考命令如下：

```
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip address 192.168.x.62 255.255.255.192
RTA(config-if)#no shutdown
RTA(config-if)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip address 10.x.1.1 255.255.255.248
RTA(config-if)#no shutdown
RTA(config)#ip route 0.0.0.0 0.0.0.0 10.x.1.2
--------其他 3 台路由器配置略--------

SWA(config)#ip routing
SWA(config)#interface FastEthernet 0/1
SWA(config-if)#no switchport
SWA(config-if)#ip address 10.x.1.2 255.255.255.248
SWA(config-if)#exit
--------接口 Ethernet 1/0/2、Ethernet 1/0/3、Ethernet 1/0/4 配置略--------
SWA(config)#interface FastEthernet 0/24
SWA(config-if)#no switchport
SWA(config-if)#ip address 10.0.x.2 255.255.255.0
SWA(config-if)#exit
SWA(config)#ip route 0.0.0.0 0.0.0.0 10.0.x.1
```

配置完成后，在 4 台路由器上使用 ping 命令测试与外部网络的联通性，应该可以 ping 通。但需要注意此时 PC_1～PC_4 均无法联通外部网络，因为交换机 SWA 并不知道 PC 所在网段的存在。在实际网络应用中也是如此，需要进行地址转换的内部网络对外部网络而言是透明的(或者说是不存在的)，外部网络不会知道使用私有 IP 地址的内部网络的存在，以防止私有 IP 地址在公共合法网络上的泄露。

(3) 在 PC_1～PC_4 上启动 XAMPP 软件，开启 Apache 服务，保证 HTTP 服务可以正常运行。

(4) 在路由器上进行 NAT 的配置，要求将路由器连接 PC 的网段中的第一个可用 IP 地址静态转换到路由器与交换机相连的网段中最后一个可用 IP 地址上，使外部网络可以主动访问 PC 上的 HTTP 服务。对于路由器连接 PC 的网段中的其他地址使用 Easy IP 进行转换，使内网主机可以访问外部网络。

H3C 设备参考命令如下：

```
[RTA]nat static 192.168.x.1 10.x.1.6
[RTA]acl number 2000
[RTA-acl-basic-2000]rule deny source 192.168.x.1 0
[RTA-acl-basic-2000]rule permit source 192.168.x.0 0.0.0.63
[RTA-acl-basic-2000]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]nat outbound static
```

```
[RTA-Ethernet0/1]nat outbound 2000
--------其他 3 台路由器配置略--------
```

Cisco 设备配置如下：

```
RTA(config)#ip nat inside source static 192.168.x.1 10.x.1.6
RTA(config)#access-list 1 deny host 192.168.x.1
RTA(config)#access-list 1 permit 192.168.x.0 0.0.0.63
RTA(config)#ip nat inside source list 1 interface FastEthernet 0/1 overload
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip nat inside
RTA(config-if)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip nat outside
--------其他 3 台路由器配置略--------
```

注意：在进行 Easy IP 使用的 ACL 的配置中，对于不需要进行 Easy IP 转换的内部本地地址要首先 deny 掉。

配置完成后，在 PC_5 的 IE 中分别输入 PC_1～PC_4 的内部全局地址来访问其上的 HTTP 服务，应该可以访问。在进行访问的同时，在 4 台路由器上使用命令 debugging nat packet 或者 debug ip nat 查看地址转换的过程，并使用命令 display nat session 或者 show ip nat translations 查看 NAT 会话情况。

(5) 将 PC_1 和 PC_2 划分到一组，PC_3 和 PC_4 划分到一组，将 PC_2/PC_4 的 IP 地址修改为相应网段中非第一个地址的任意合法地址，例如第二个地址，然后在 PC_2 和 PC_4 的 IE 中分别输入同组的 PC_1 或 PC_3 的内部全局地址来访问其上的 HTTP 服务，应该可以访问。在进行访问的同时，在 4 台路由器上使用命令 debugging nat packet 或者 debug ip nat 查看地址转换的过程，并使用命令 display nat session 或者 show ip nat translations 查看 NAT 会话情况。

注意：在 PC_2/PC_4 访问同组的 PC_1/PC_3 的 HTTP 服务过程中，实际上经过两次地址转换，分别为在路由器 RTB/RTD 上进行的 Easy IP 的转换，以及在路由器 RTA/RTC 上进行的静态地址转换。具体如图 3-10 所示。

5. 实验报告

NAT 配置	RTA				
	RTB				
	RTC				
	RTD				
PC_2 访问 PC_1 的 HTTP 服务时 display nat session 结果		InsideAddr	Port	GlobalAddr	Port
	RTA				
	RTB				
PC_4 访问 PC_3 的 HTTP 服务时 display nat session 结果		InsideAddr	Port	GlobalAddr	Port
	RTC				
	RTD				

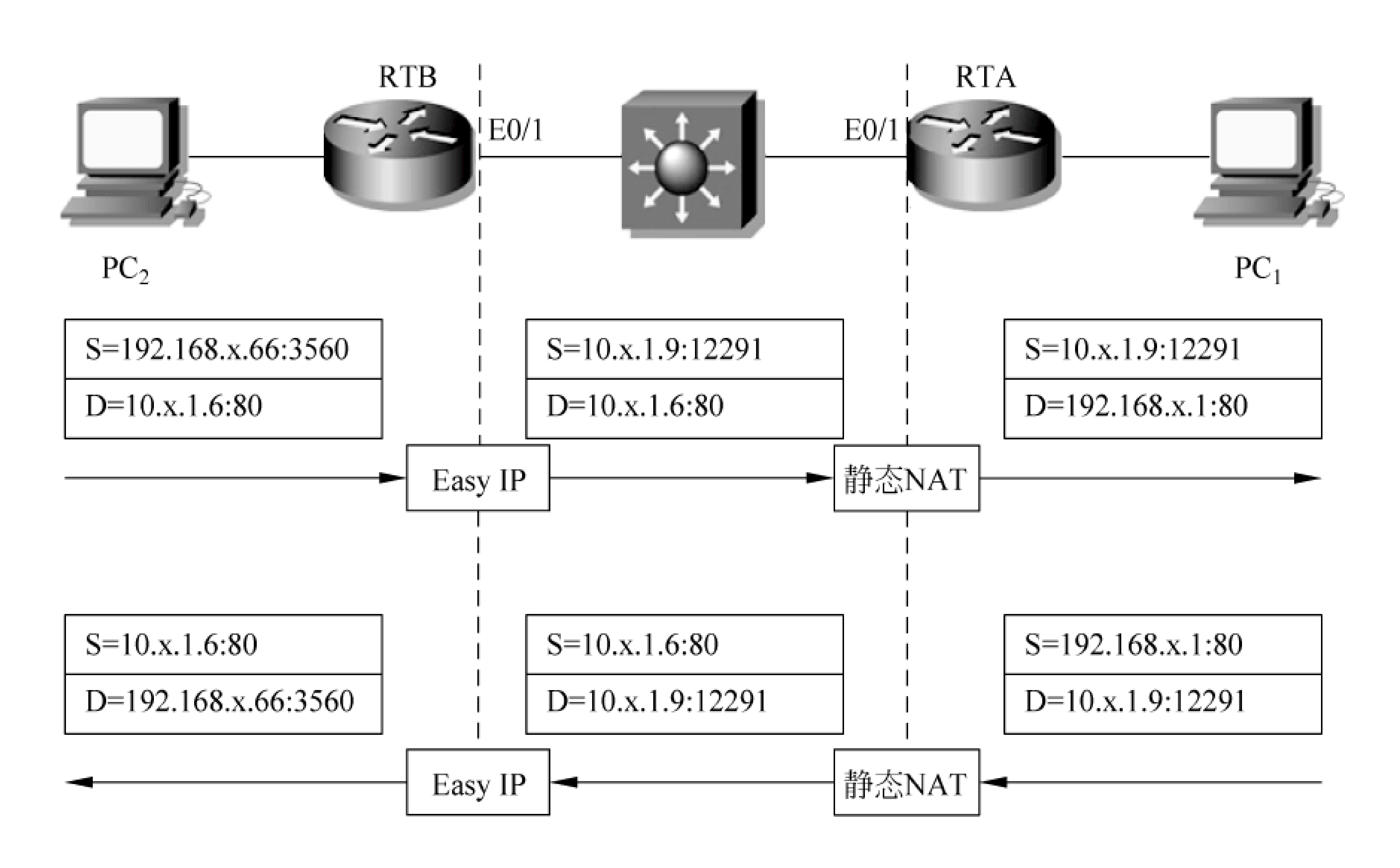


图 3-10 两次地址转换过程

3.13.2 NAT Server 与 Easy IP 配置及验证实训

实验学时：4 学时。

每组实验学生人数：4 人。

1. 实验目的

(1) 掌握 NAT Server 和 Easy IP 的配置方法。

(2) 理解 NAT Server、Easy IP 以及 NAT ALG 的工作原理及转换过程。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：5 台

(2) 路由器：4 台

(3) 三层交换机：1 台

(4) 二层交换机：1 台

(5) UTP 电缆：11 条

(6) Console 电缆：5 条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 配置 NAT Server。

(2) 配置 Easy IP。

(3) 查看并分析 NAT ALG 的工作过程。

4. 实验指导

本次实验依然使用 3.13.1 小节的网络拓扑结构。

(1) 参考 3.13.1 小节实验指导步骤(1)。

(2) 参考 3.13.1 小节实验指导步骤(2)。

(3) 在 PC_1～PC_4 上启动 XAMPP 软件,开启 File Zilla 服务,保证 FTP 服务可以正常运行。

(4) 在路由器上配置 NAT Server,要求外部网络通过路由器 E0/1 接口的 IP 地址可以访问到内部网络中第一个可用 IP 地址主机上的 FTP 服务;在路由器上配置 Easy IP,使内网主机可以访问外部网络。

H3C 设备参考命令如下:

```
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]nat server protocol tcp global 10.x.1.1 21 inside 192.168.x.1 21
[RTA-Ethernet0/1]nat server protocol tcp global 10.x.1.1 20 inside 192.168.x.1 20
Error: Can't use ftp's data connection!
[RTA-Ethernet0/1]nat outbound
--------其他 3 台路由器配置略--------
```

Cisco 设备参考命令如下:

```
RTA (config)#ip nat inside source static tcp 192.168.x.1 21 10.x.1.1 21
RTA (config)#ip nat inside source static tcp 192.168.x.1 20 10.x.1.1 20
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip nat inside
RTA(config-if)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip nat outside
```

在上面的配置中应注意以下两点。

① 对于 Easy IP 而言,如果所有的内网 IP 地址均需要进行转换,则不需要定义 ACL 去限定内部本地地址的范围。

② 在 H3C 设备上不能、也不需要对 FTP 的数据端口 20 进行 NAT Server 的配置,因为在内部网络存在 FTP 服务器的时候,如果外网主机使用被动模式访问 FTP 服务器,则在 FTP 服务器对外网主机的 PASV 请求报文的响应报文中会包含自己的 IP 地址和监听的端口,这个处于应用层报文中的 IP 地址和端口会在路由器上由 NAT ALG 技术转换为合法公有的 IP 地址以及相应的端口,从而保证外网主机可以访问内部网络的 FTP 服务器;如果外网主机使用主动模式访问 FTP 服务器,则由 FTP 服务器主动发起数据连接,就不再涉及 NAT ALG 技术,NAT Server 技术会自动为 FTP 服务器的数据端口进行一个类似 Easy IP 的转换,保证外网主机可以访问内部网络的 FTP 服务器。

配置完成后,在 PC_5 的 IE 中分别输入 4 台路由器 E0/1 接口的 IP 地址来访问 PC_1～PC_4 上的 FTP 服务(被动模式访问),可以访问。在进行访问的同时,在 PC_5 和进行访问的相应 PC 上分别使用 Wireshark 软件捕获 FTP 的数据报文,查找其中包含数据连接 IP 地址和端口的协商报文,并进行比对,理解 NAT ALG 技术对多通道协议应用层数据的处理。在 4 台路由器上使用命令 debugging nat packet 或者 debug ip nat 查看地址转换的过程,并使用命令 display nat session 或者 show ip nat translations 查看 NAT 会话情况。

在 PC_5 使用被动模式访问 PC_1 上的 FTP 服务时,分别在 PC_1 和 PC_5 上使用 Wireshark 软件捕获的 FTP 数据报文如图 3-11 和图 3-12 所示。

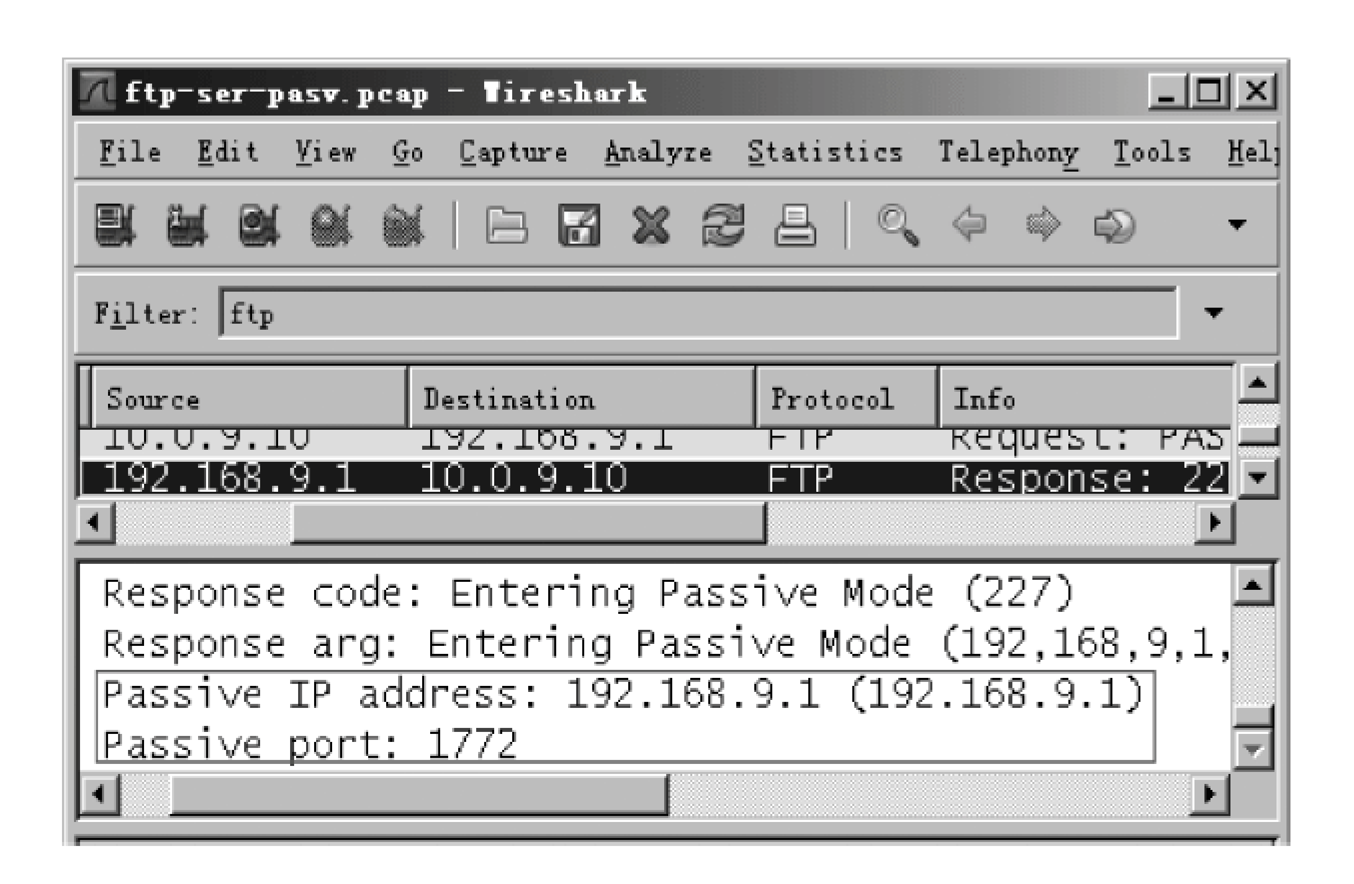


图 3-11　PC_1 上的 FTP 报文

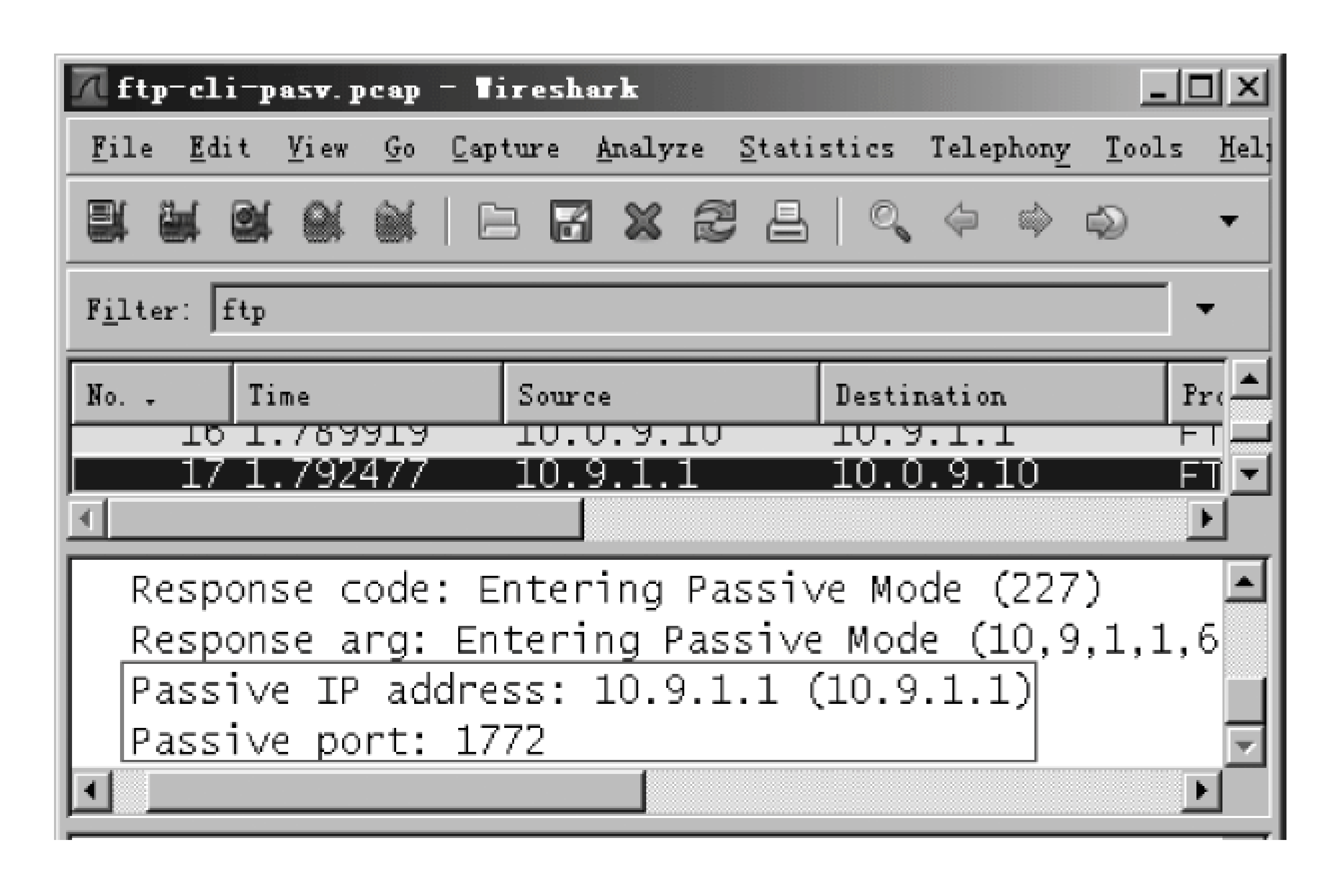


图 3-12　PC_5 上的 FTP 报文

(5) 将 PC_1 和 PC_2 划分到一组，PC_3 和 PC_4 划分到一组，在 PC_2 和 PC_4 的 IE 中分别输入路由器 RTA 和 RTC 的 E0/1 接口 IP 地址访问同组的 PC_1 和 PC_3 上的 FTP 服务，无论使用主动模式还是使用被动模式均可以访问。

在使用被动模式进行访问时，将在路由器 RTA 和 RTC 上通过 NAT ALG 技术将 FTP 服务器对 PASV 请求报文的响应报文中包含的 IP 地址和监听的端口进行转换，这一点在步骤(4)中进行了详细介绍，在此不需要再次进行抓包分析。

在使用主动模式进行访问时，将在路由器 RTB 和 RTD 上通过 NAT ALG 技术将进行数据通道协商的 PORT 报文中包含的 IP 地址和监听的端口进行转换。在进行访问的同时，在 PC_2/PC_4 和进行访问的同组的 PC_1/PC_3 上分别使用 Wireshark 软件捕获 FTP 的数据报文，查找其中包含数据连接 IP 地址和端口的协商报文，并进行比对，理解 NAT ALG 技术对多通道协议应用层数据的处理。在 4 台路由器上使用命令 debugging nat packet 查看地址转换的过程，并使用命令 display nat session 查看 NAT 会话情况。

在 PC_2 使用主动模式访问 PC_1 上的 FTP 服务时，分别在 PC_2 和 PC_1 上使用 Wireshark 软件捕获的 FTP 数据报文如图 3-13 和图 3-14 所示。

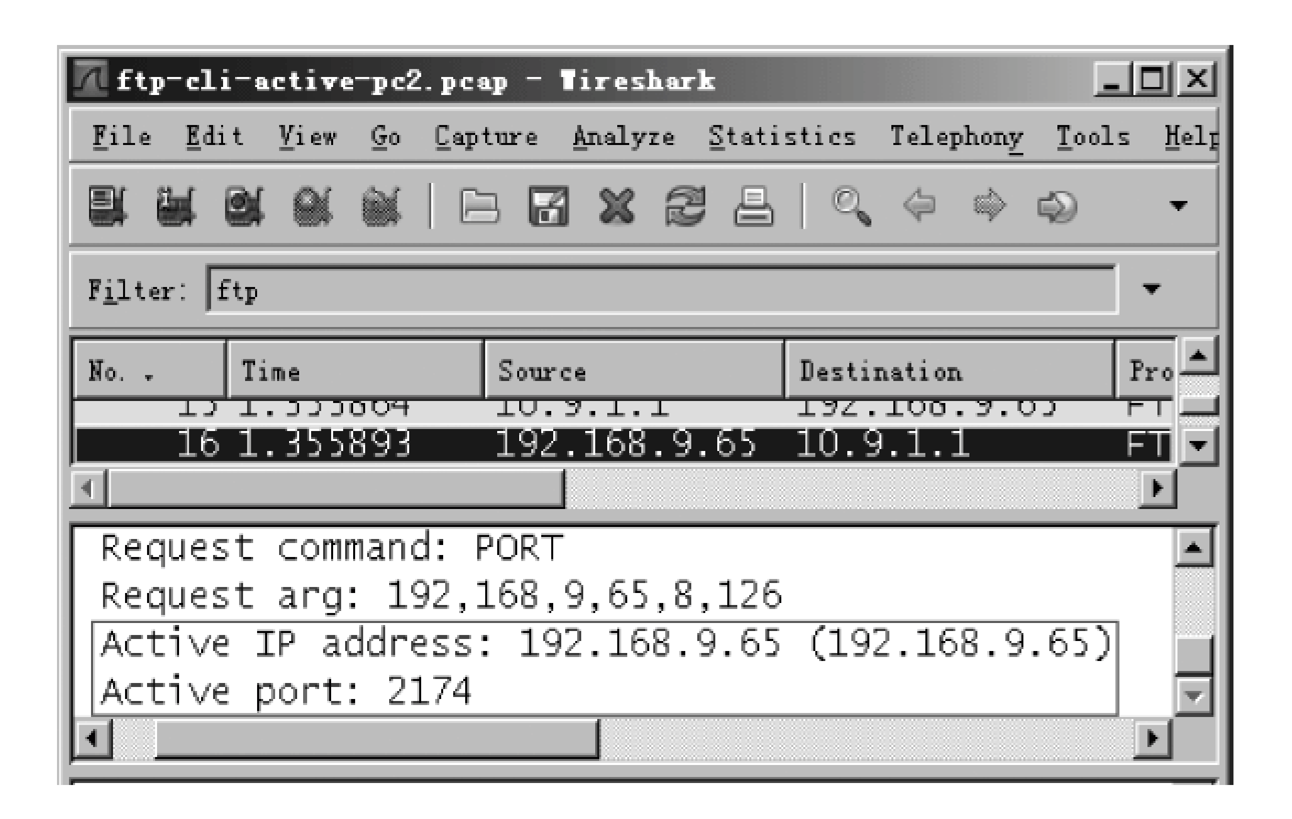


图 3-13 PC$_2$ 上的 FTP 报文

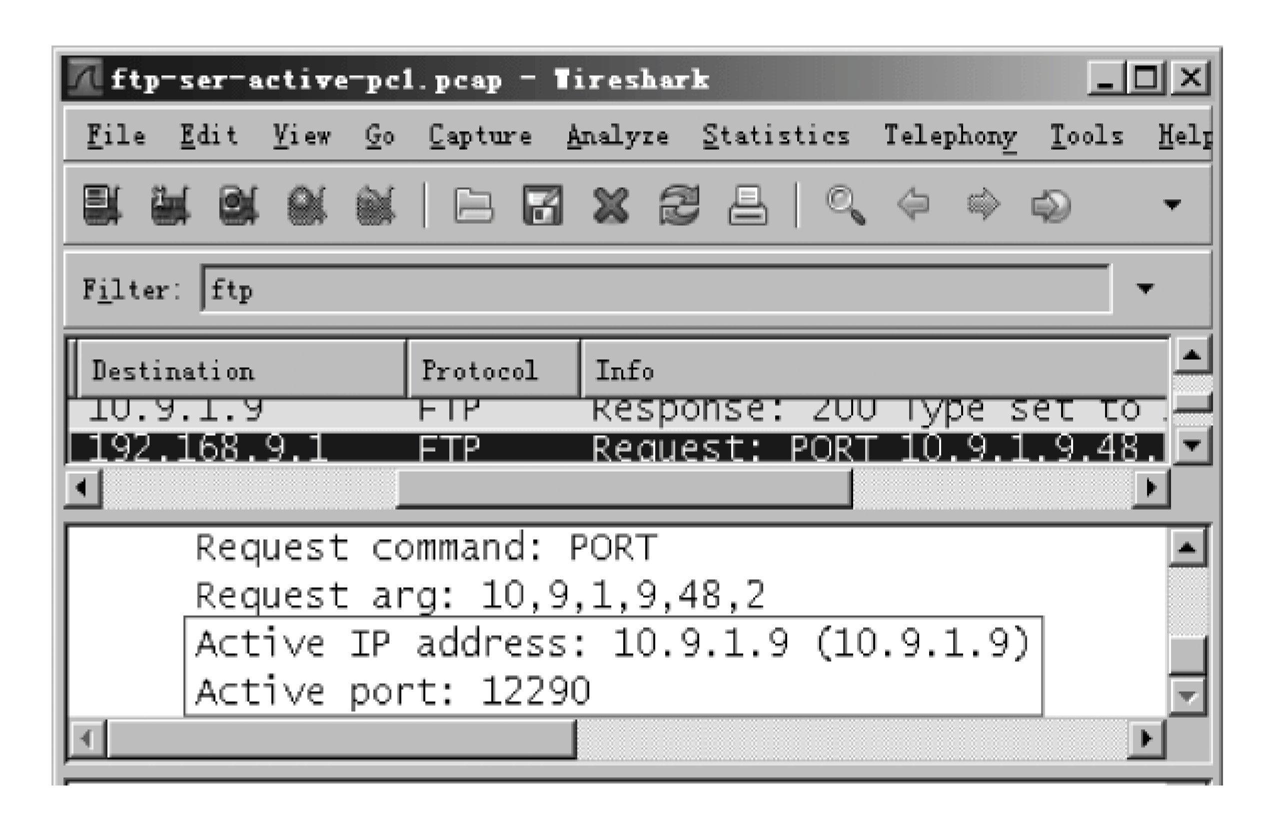


图 3-14 PC$_1$ 上的 FTP 报文

在 PC$_2$/PC$_4$ 访问 PC$_1$/PC$_3$ 上的 FTP 服务的过程中，涉及了 Easy IP、NAT Server 和 NAT ALG 3 种不同的地址转换技术。报头中的 IP 地址和端口使用 Easy IP 和 NAT Server 技术经过了两次地址转换，应用层报文中的 IP 地址和端口使用 NAT ALG 进行了地址转换。整个访问过程相对比较复杂，请尝试给出主动/被动两种不同模式下进行 FTP 访问时地址转换的整个过程。

5. 实验报告

NAT 配置	RTA					
	RTB					
	RTC					
	RTD					
PC$_5$ 使用被动模式访问 PC$_1$～PC$_4$ 的 FTP 服务时抓包结果		Passive IP address	Passive port		Passive IP address	Passive port
	PC$_1$			PC$_5$		
	PC$_2$			PC$_5$		
	PC$_3$			PC$_5$		
	PC$_4$			PC$_5$		

续表

PC_2/PC_4 使用主动模式访问 PC_1/PC_3 的 FTP 服务时抓包结果		Active IP address	Active port		Active IP address	Active port
	PC_2			PC_1		
	PC_4			PC_3		
PC_2/PC_4 使用主动模式访问 PC_1/PC_3 的 FTP 服务时地址转换过程						
PC_2/PC_4 使用被动模式访问 PC_1/PC_3 的 FTP 服务时地址转换过程						

第 4 章

VPN 技术

本章任务：根据工程任务安全需求分析，解决利用 Internet 线路进行安全通信配置问题。

必备知识：（1）VPN 概念。

（2）站到站 VPN 配置。

（3）远程访问 VPN 配置。

学习目标：完成在路由器上创建模拟分公司与分支机构间、分支机构与员工 PC 间 VPN 连接的配置任务，保护基于 Internet 线路的网络通信安全。

4.1 模拟公司网络安全通信配置任务分析

如图 4-1 所示，模拟分公司 1 与分支机构 B-1 间租用 Internet 线路进行通信。为保证公司网络通信安全，应达到以下要求。

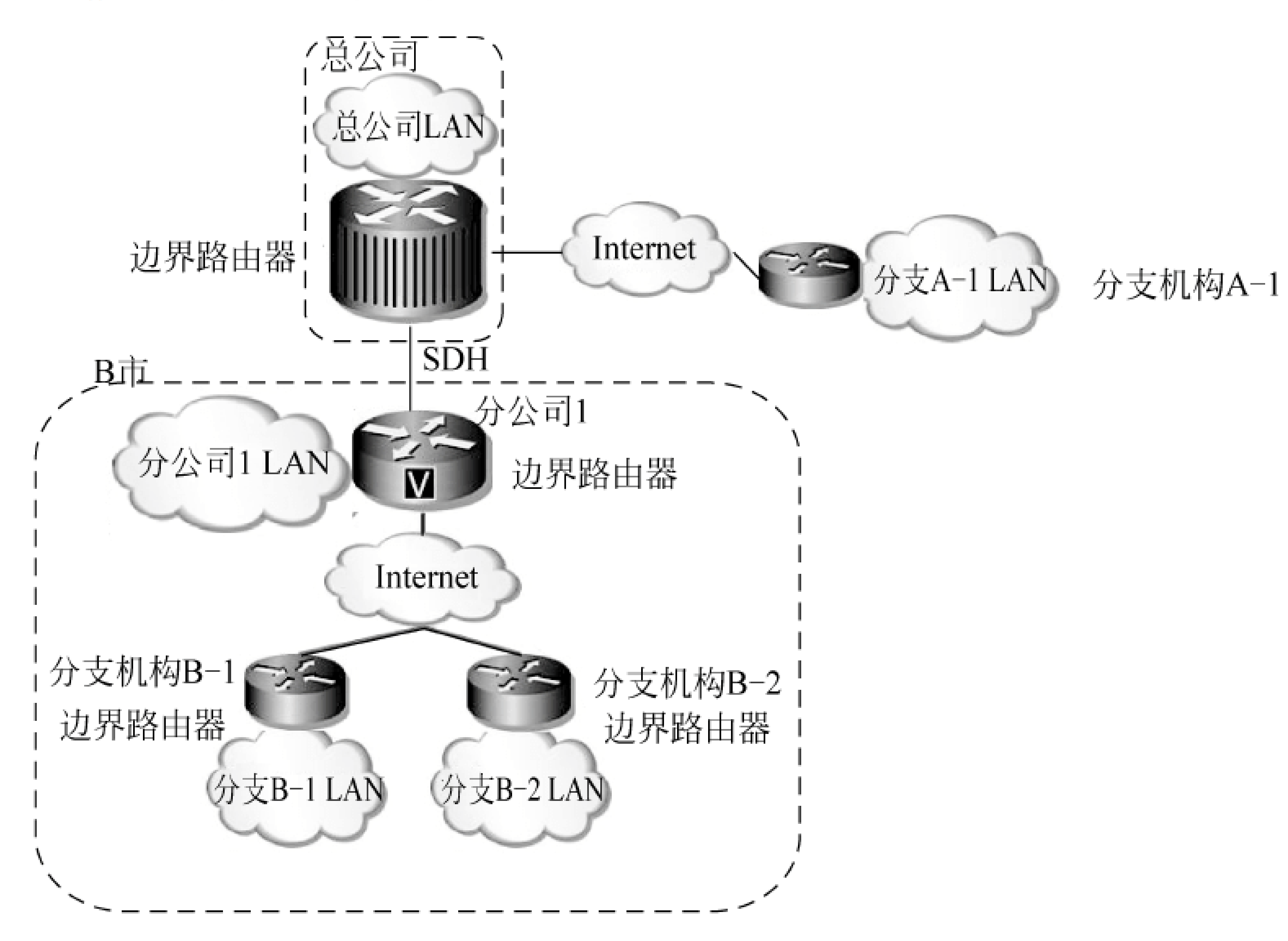


图 4-1 分支机构 B-1 与公司其他单位间的网络连接

（1）凡是分支机构 B-1 与模拟分公司 1 间的通信都要受到加密保护。

（2）公司职员在 Internet 上对分支机构 B-1 内服务器的远程访问受到加密保护。

更进一步，要求公司所有使用 Internet 线路的网络间进行通信时，均应受到加密保护。

4.2　VPN 基础

面对诸多的网络威胁和攻击，数据以明文的方式在公共网络上进行传输的时候，很容易遭到恶意攻击者的窃听或者篡改。为保障数据在公共网络上传递的安全性，产生了虚拟专用网（Virtual Private Network，VPN）技术。VPN 技术通过使用加密、认证等技术，为用户在公共网络上提供像专用网络一样的通信保障。

在网络通信中，要保障数据在传递过程中的安全性，必须要满足如下 3 点基本安全需求。

（1）数据的机密性。所谓机密性（Confidentiality）是指防止数据被未经授权的恶意窃听者所理解，以保障在存储和传输的过程中数据内容不被泄露。

（2）数据的完整性。数据完整性（Data Integrity）是指防止数据在存储和传输的过程中被非法篡改，包括无权者的篡改、有限权限者的越权篡改以及存储传输中的意外导致的错误。

（3）数据发送者的身份真实性。数据发送者的身份真实性是指数据接收者应能够验证数据来自正确的发送者，而不是由恶意攻击者伪造，另外数据发送者的身法验证还具备反拒认（Nonrepudiation）功能，即数据发送者不能否认自己曾发送过数据。

下面分别就以上 3 点安全需求对相关基础知识进行介绍。

4.2.1　数据加密技术

一般在网络中传输的数据都没有进行加密处理，此时的数据称之为明文，一旦被恶意攻击者窃听，内容就会泄露。为保障数据的机密性就需要对数据加密，加密技术可以分为加解密密钥和加解密算法两部分，加解密密钥是在加解密过程中使用的一串数字，作为一个运算参数出现；加解密算法是作用于加密密钥和明文或者解密密钥和密文的一个数学函数。使用加密算法对加密密钥和明文运算得到的结果即为数据的密文。根据加密算法工作方式的不同，可以将加密技术分为对称加密技术和非对称加密技术两种。

1. 对称加密技术

对称加密技术又称为秘密密钥加密技术，在对称加密技术中，通信双方共享同一个密钥，加解密均使用该唯一的密钥来实现，如图 4-2 所示。

常见的对称加密算法有数字加密标准（Digital Encryption Standard，DES）、三重 DES（Triple DES）和高级加密标准（Advanced Encryption Standard，AES）等算法。

DES 算法使用 64bit 的密钥将 64bit 的明文数据块加密产生 64bit 的密文。在 64bit 的密钥中，其中 56bit 是随机生成的（即密钥本身），其余 8bit 为数据校验位，每一位校验

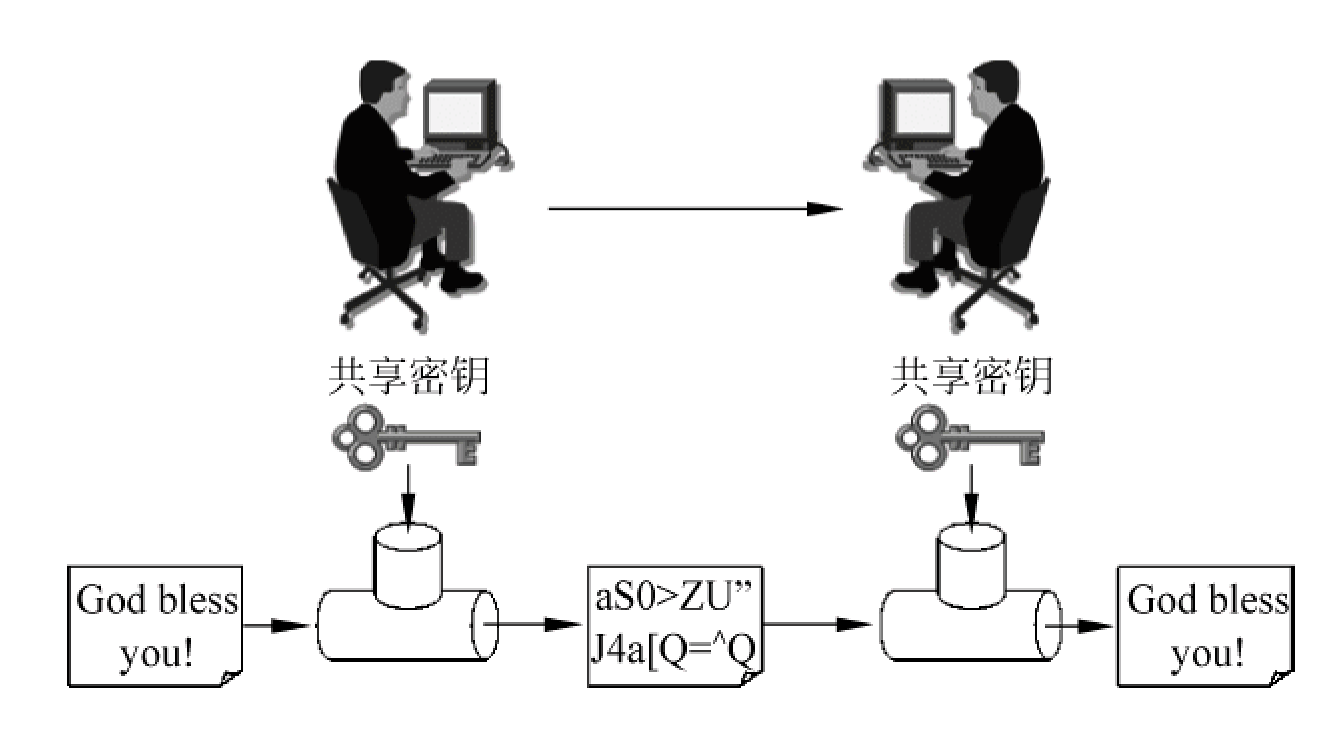


图 4-2 对称加密技术

位对 56bit 的随机值中的一个 7bit 块进行校验。

3DES 算法是一种更安全的 DES 算法的变种,随着计算机运算能力的增强,DES 算法的密钥变得容易被暴力破解,在这种情况下出现了 3DES 算法。3DES 算法使用 3 个 56bit 的密钥对数据进行 3 次 DES 加密来保障数据的机密性,如果 3 个密钥互不相同,就相当于使用了一个 168bit 的密钥对数据进行加密。3DES 算法是 DES 算法向 AES 算法过渡的一种加密标准。

AES 算法又称为 Rijndael 算法,它能够提供比 DES 更强的抗攻击能力,并将最终取代 DES 算法。AES 算法采用分组密码体制,密钥长度和进行加密的明文数据块可以是 128bit、192bit 或 256bit 中的任意一个。AES 使用多轮的重复和变换来提高数据的抗攻击能力。

对称加密算法速度快、效率高,适合于对大量的数据、动态的数据流进行加密。但对称加密算法的安全性在相当大的程度上依赖于共享密钥本身的安全性。一旦共享密钥被第三方获知就会造成数据的失密。共享密钥的泄露存在如下两方面的原因:

(1) 由于通信双方使用同一个密钥进行加解密,因此在进行加解密之前就需要在通信双方之间传递共享密钥,而在不安全的通信通道上进行密钥交换时有可能造成共享密钥的泄露。

(2) 密钥一般都会有安全的时效性,静态配置的密钥只能提供暂时的安全性,随着时间的推移,密钥泄露的可能性也会逐渐增大。另外,如果采用静态配置的共享密钥,N 个用户之间进行通信时,每一个用户都需要维护($N-1$)个共享密钥,增加了密钥管理的复杂度。

2. 非对称加密技术

非对称加密技术又称为公开密钥加密技术,它为每一个用户分配一对密钥:其中一个密钥是保密的,由用户自己保管,称之为私钥;另外一个密钥是公开的,称之为公钥。这一对密钥互为加/解密密钥,即由公钥加密的数据可以由私钥来解密,而由私钥加密的数据可以由公钥来解密。但是由其中一个密钥无法计算出另一个密钥。非对称加密技术的实现如图 4-3 所示。

在使用非对称加密技术对数据进行加密时,发送方使用接收方的公钥对数据进行加

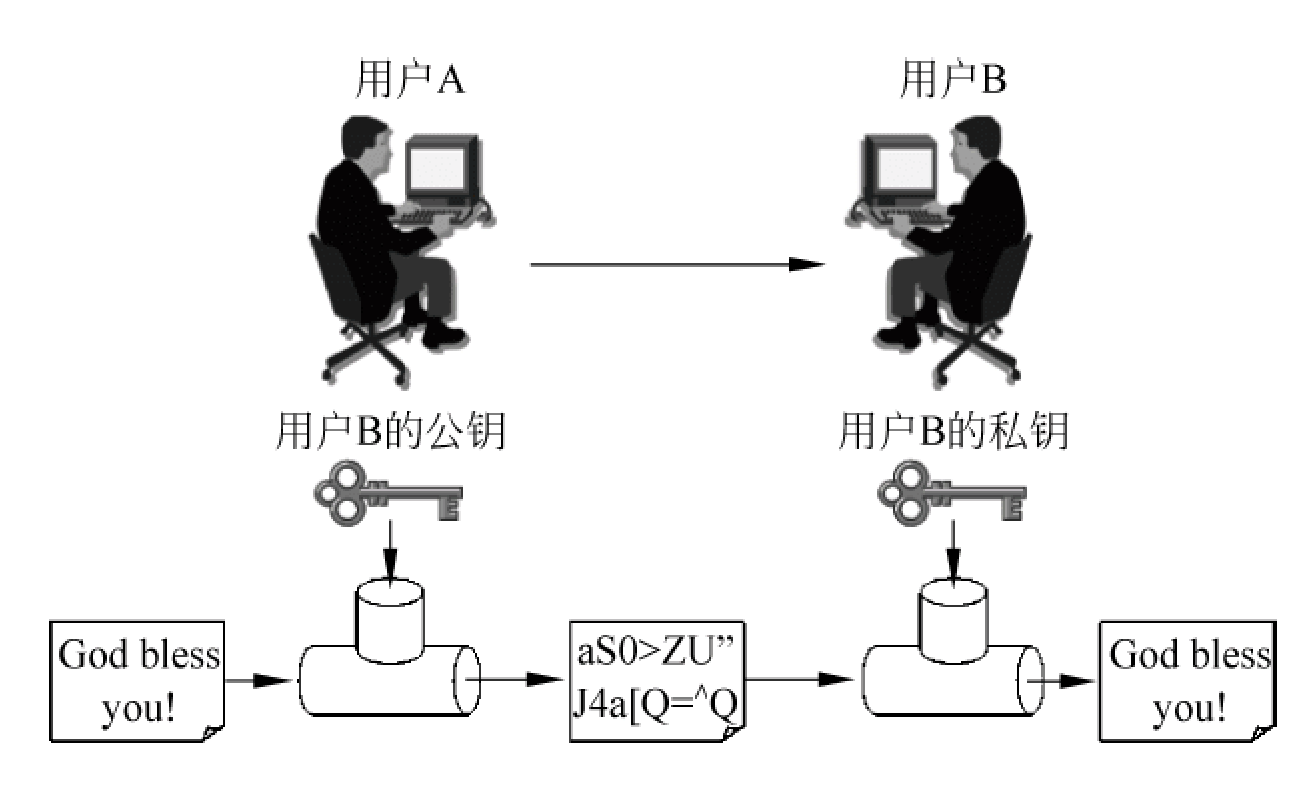


图4-3 非对称加密技术

密,接收方在接收到密文数据后,使用自己的私钥对数据进行解密。

目前最流行的非对称加密算法是RSA(Rivest-Shamir-Adelman)算法,RSA算法由Ron Rivest、Adi Shamir和Leonard Adelman共同开发,它的原理基于一个非常简单的事实:将两个大素数相乘十分容易,但想要对其乘积进行因式分解却极其困难。

非对称加密算法由于不再需要维护共同的共享密钥,不必担心密钥的泄露,因此非对称加密算法降低了密钥管理的复杂度,并且提供了更好的安全性。但是非对称加密算法加密效率非常低,RSA算法一般要比DES算法慢1000倍左右,因此非对称加密算法很少被应用在数据加密领域,它实际上被更多地应用在数字签名以及密钥的交换和管理中。

3. D-H算法

由于非对称加密算法效率低下,因此在IPSec VPN中实际上使用的是对称加密算法来保障数据的机密性。但是对称加密算法又存在共享密钥容易泄露的问题。为了解决这个问题,一方面使用一次性密钥,即每次通信都更换新的密钥来保障密钥的安全;另一方面就需要设法使共享密钥可以在不安全的通信通道上进行安全的传递,解决方法就是使用Diffie-Hellman(D-H)算法来实现。D-H算法的工作原理如图4-4所示。

具体的密钥交换步骤如下。

(1)首先有两个全局公开的参数。素数p和p的一个原根a,这两个参数可以由其中一个用户选择产生并封装在第一个报文中告诉对端用户。

(2)通信双方分别创建一个大的随机数X_A、X_B作为自己的私钥。

(3)通信双方分别使用参数p、a和自己的私钥计算生成自己的公钥Y_A和Y_B,并将自己的公钥传递给对端用户。

(4)通信双方分别使用参数p、对端的公钥和自己的私钥运算产生相同的结果K。

(5)通信的一方产生一个临时密钥T作为共享密钥,并使用上一步的计算结果K作为密钥对其进行加密。

(6)通信的另一方接收到加密后的共享密钥后,使用K对其进行解密得到共享密钥T。

(7)通信双方使用共享密钥T和对称加密算法对数据进行加密和解密,确保数据在

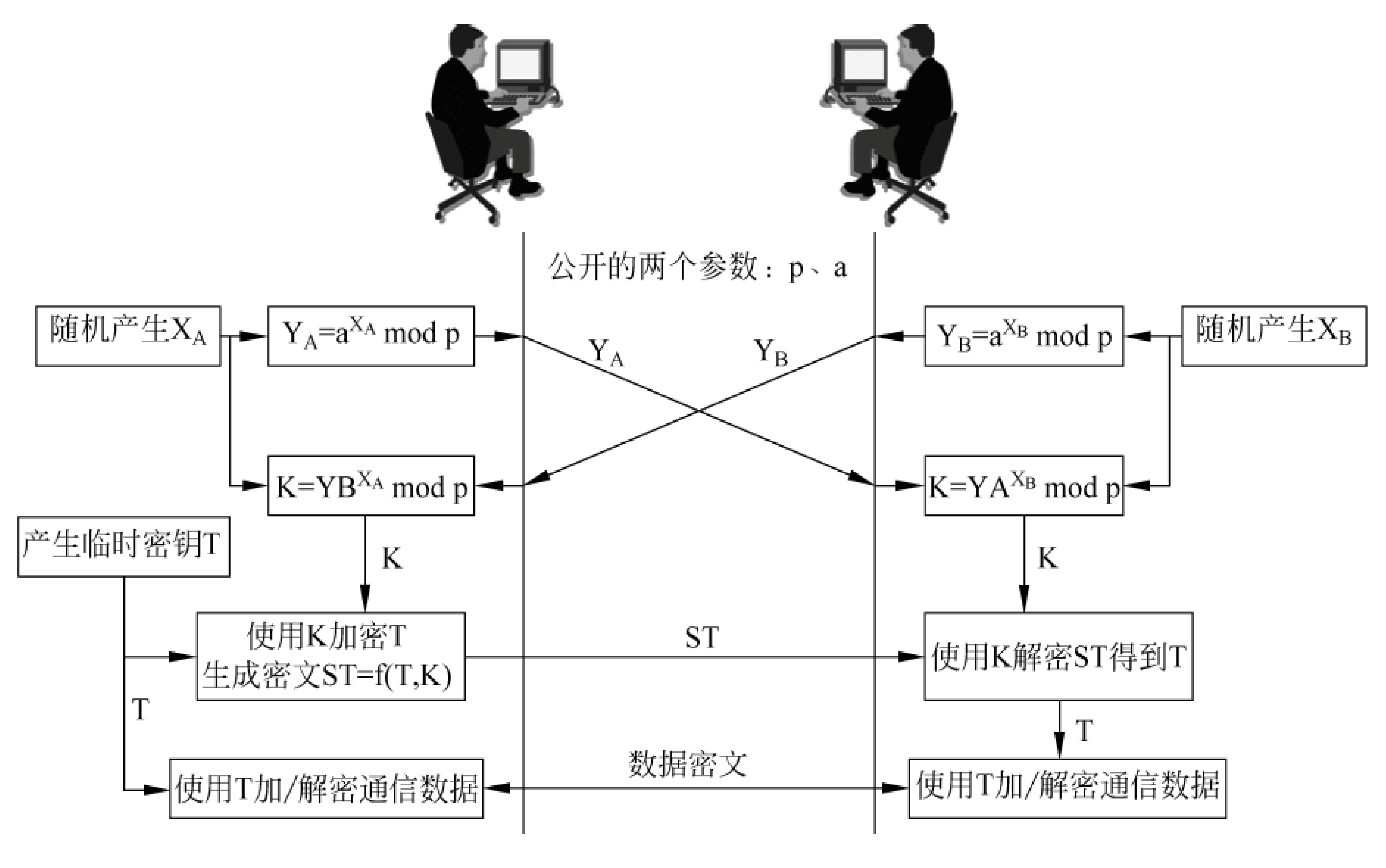


图 4-4 D-H 算法

网络中传输的机密性。

在 D-H 算法进行密钥交换的过程中，公开交换了参数 p、a、Y_A 和 Y_B，但是使用这4个参数并不能计算出通信双方的私钥 X_A 和 X_B，也无法计算出 K，从而保证了一次性共享密钥 T 的安全传递。D-H 算法实际上就是使用非对称加密技术来保障一次性对称密钥交换的安全性。

D-H 算法只能用于进行密钥的交换，不能用于数据加密和数字签名等其他目的。另外，D-H 算法存在如下几点不足。

(1) D-H 算法没有提供通信双方的身份信息，无法对对端用户的身份进行认证，因此容易遭受中间人攻击，解决的方法是在 D-H 消息交换的过程中使用数字证书进行身份认证。

(2) 由于 D-H 算法的计算密集性，导致其容易受到拒绝服务攻击，即攻击者请求大量的密钥，导致被攻击者花费大量的计算资源求解无用的幂系数。

(3) D-H 算法无法防止重放攻击。

4.2.2 数据完整性保证

为保证数据的完整性，通信的接收方应该可以对接收到的数据进行验证，以便发现数据在传输过程中是否遭到了篡改，而验证数据完整性一般使用散列算法来实现。

1. 散列算法

散列(Hash)算法是一种单向函数，它将任意长度的输入通过计算产生一个固定长度的输出，这个输出称为摘要或者散列值。散列算法具备如下特点。

(1) 对同一源数据反复进行散列运算得出的散列结果总是相同。

(2) 对源数据的一个细小的修改都会导致产生完全不同的散列值。

(3) 由于在散列的过程中损失了信息，因此散列具有不可逆性，即无法通过生成的散列值计算出源数据。

使用散列算法保障数据完整性的过程如图 4-5 所示。

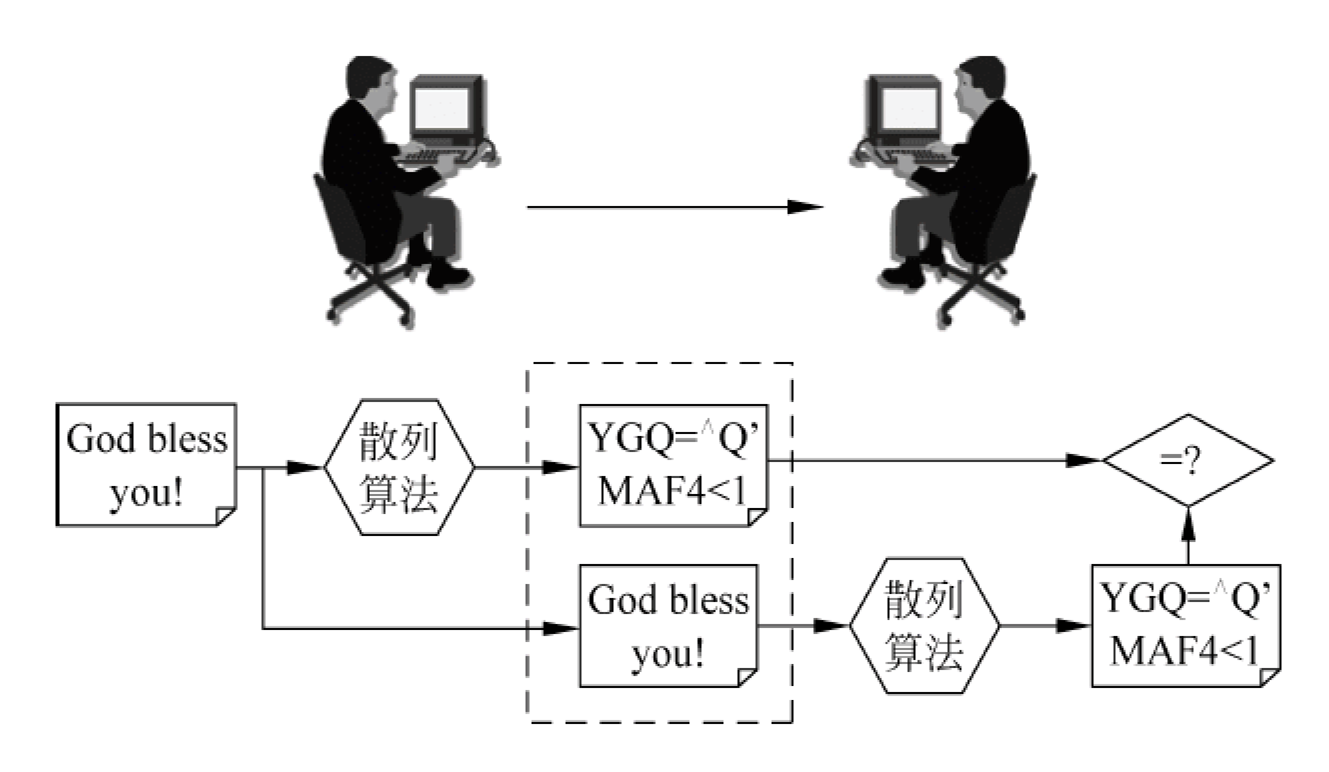


图 4-5　数据完整性验证

发送方在进行数据发送之前，首先使用散列算法计算出源数据的散列值，然后将源数据及其散列值一并发送给接收方；接收方接收到数据后，对接收到的数据使用相同的散列算法计算出其散列值，并和收到的散列值相比较，如果两个散列值相同，则说明数据在传输过程中未被篡改。

常见的散列算法包括消息摘要算法第 5 版(Message Digest Algorithm 5，MD5)和安全散列算法(Secure Hash Algorithm，SHA)。MD5 算法对于任意长度的输入计算产生一个 128bit 的散列值；而 SHA-1 算法对于任意长度的输入计算产生一个 160bit 的散列值。相比较而言，SHA-1 算法具有比 MD5 算法更强的抗攻击能力，但 SHA-1 算法的运算速度比 MD5 算法要慢。

散列算法还经常与数字签名结合使用来实现对发送方身份的验证、反拒认功能以及保障数据的完整性。

2. 散列消息认证码

上一节对使用散列算法保障数据的完整性进行了介绍，实际上这里会有一个问题：由于散列算法是公开的，攻击者完全可以在网络中截获源数据后对其进行篡改并重新生成散列值，将篡改后的数据和散列值发送给接收方，而接收方无法验证出其是否存在的完整性问题。对于这个问题可以使用散列消息认证码(Hashed Message Authentication Code，HMAC)技术来解决。

HMAC 技术通过加密散列来保障数据的完整性，即在使用散列算法计算散列值时加入了一个随机生成的共享密钥作为参数，如图 4-6 所示。

使用 HMAC 技术后，即使数据被恶意攻击者截获并篡改，由于没有共享密钥，攻击者无法生成正确的散列值，接收方就可以发现其中存在的完整性问题。常用的基于 HMAC 技术的的散列算法有 HMAC-MD5 和 HMAC-SHA1 两种，相对而言 HMAC-SHA1 有着更好的抗攻击强度。

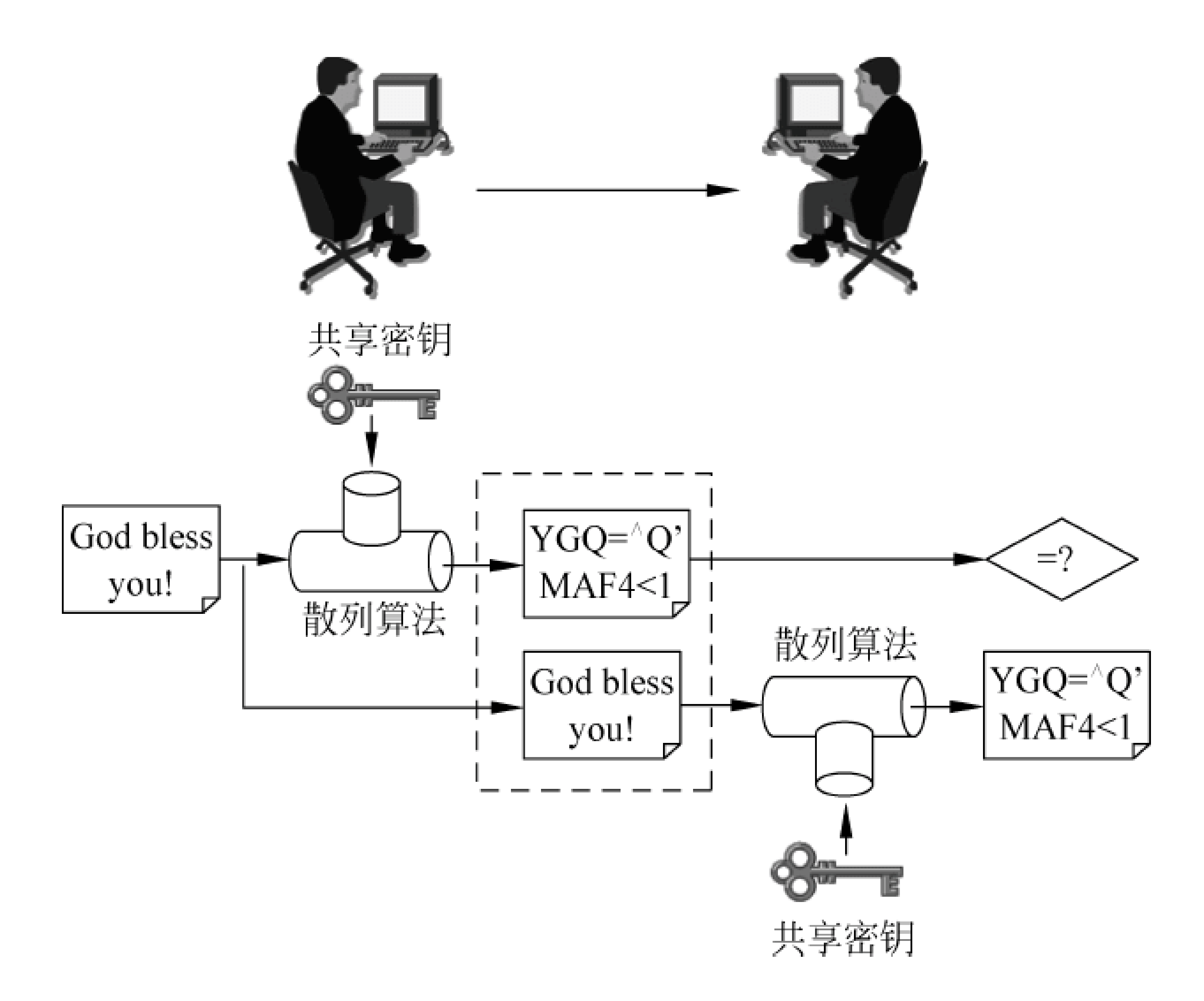


图 4-6 HMAC 过程

4.2.3 数字签名及数字证书

在现实生活中,为了确保合同或者文件的有效性,往往需要对其进行签名甚至按手印。这个签名实际上有两个作用:一方面表示签名者承认某些事实或者同意某种契约,事后不能予以否认;另一方面通过签名和指纹来对签名者身份进行验证,确保签名者身份的合法性和真实性。而在网络中同样可以通过类似的方式来保障通信数据来自合法的发送方,使用的技术被称为数字签名。

数字签名使用非对称加密技术来实现。在非对称加密技术中,两个密钥互为加/解密密钥,加密时发送方使用接收方的公钥进行加密,而接收方使用自己的私钥进行解密,由于接收方的私钥只有接收方自己知道,因此可以保障数据的机密性。而既然私钥只有用户自己知道,那能不能使用私钥来作为用户身份验证的依据呢?数字签名正是基于这样的想法来实现:发送方在发送数据时使用自己的私钥对数据进行加密,而接收方使用发送方的公钥进行解密,如果接收方可以对数据进行正常解密,就验证了发送方身份的真实性,数字签名的过程如图 4-7 所示。

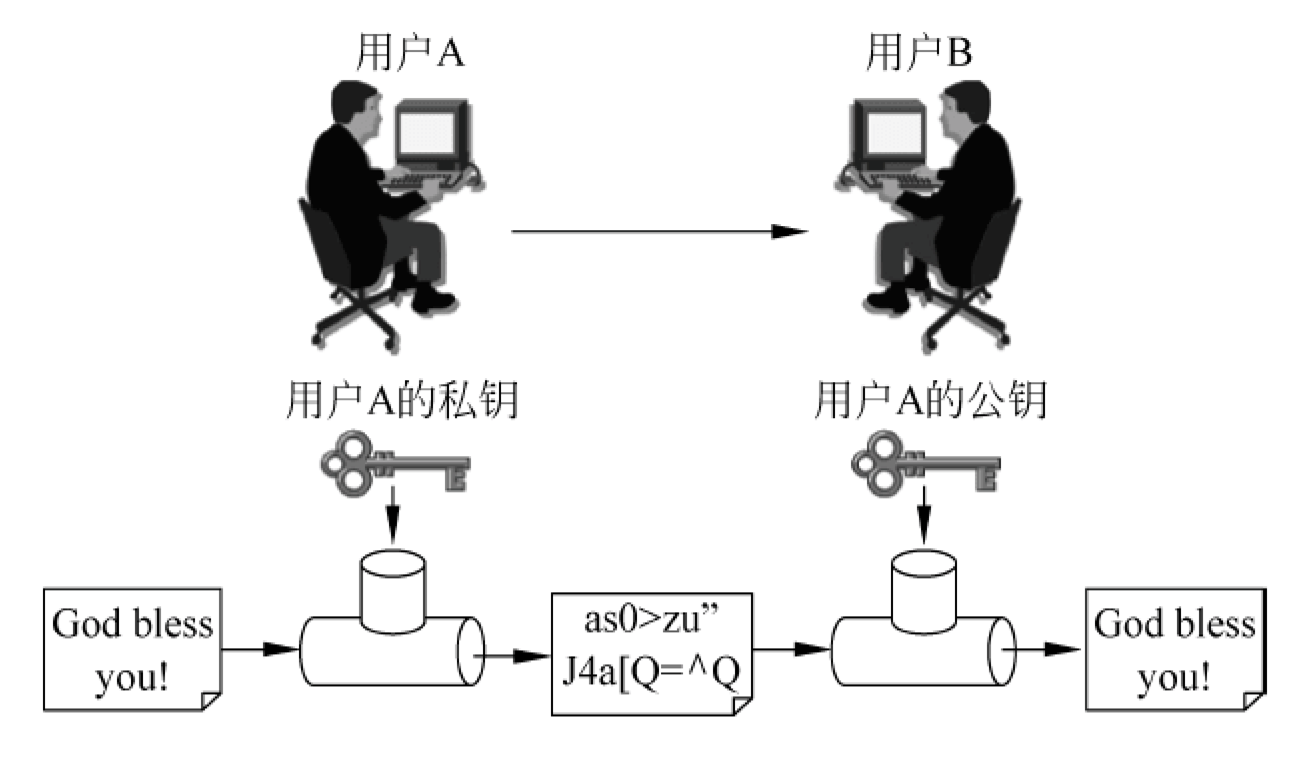


图 4-7 数字签名 1

通过图 4-7 所示的数字签名过程实现了对发送方身份的验证，但是这里会有一个问题：由于非对称加密算法效率非常低，如果对大量的数据进行数字签名，岂不是会使系统效率受到非常大的影响？在 4.2.2 小节中对散列算法进行了介绍，而散列算法的特点决定了散列值对于源数据的唯一性，而且散列值相对于源数据要小了很多，因此在实际应用中数字签名是通过对源数据的散列值进行签名来实现的。在统计上可以认为对源数据的散列值进行签名和对源数据本身进行签名是等效的，数字签名的实际实现过程如图 4-8 所示。

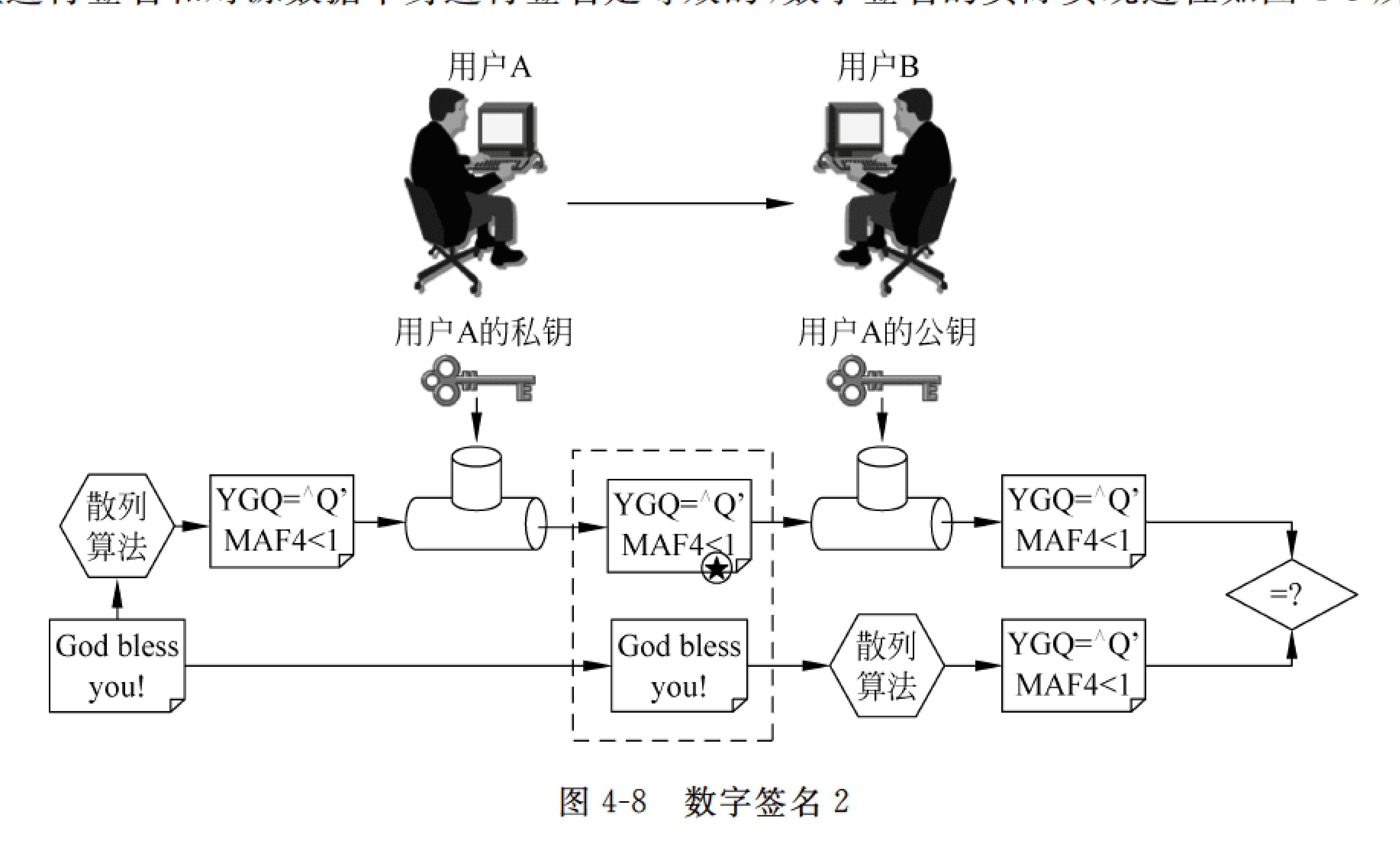


图 4-8　数字签名 2

具体的步骤如下：

(1) 发送方用户 A 使用散列算法计算出源数据的散列值，并使用自己的私钥对散列值进行签名。

(2) 用户 A 将源数据和经过签名的散列值通过网络发送给接收方用户 B。

(3) 用户 B 使用用户 A 的公钥对接收到的经过用户 A 签名的散列值进行解密，得出原始的散列值。

(4) 用户 B 使用与用户 A 相同的散列算法计算出接收到的源数据的散列值。

(5) 将两个散列值进行比较，判断是否相同。如果两个散列值相同，则一方面对发送方用户 A 的身份进行了验证，另一方面也保障了数据的完整性。

目前常用于进行数字签名的算法包括数字签名算法(Digital Signature Algorithm, DSA)和前面介绍过的 RSA 算法。DSA 算法的安全性与 RSA 算法类似，但 DSA 算法只用于进行数字签名，而一般不用于进行数据加密。

通过数字签名对发送方的身份进行验证，但这个验证很可能会出现问题，例如恶意攻击者冒充合法发送方在网络上发布自己的公钥达到身份欺骗的目的。就像在现实生活中，签名是可以模仿的。在现实生活中为防止冒充身份伪造签名，可以在签名时查看签名者由公安局核发的身份证以确认其身份。在数字签名中采用了类似的方法，即数字证书技术。

与身份证类似，数字证书由通信双方都信赖的第三方认证中心(Certificate Authority, CA)签署发放，用于进行用户的身份认证。数字证书实际上就是一串包含用

户身份信息、用户公钥以及CA数字签名的字符串,其主要内容如下:

(1)证书的序列号。

(2)证书的有效期。

(3)证书颁发机构的名称。

(4)证书申请者的名称、组织机构信息或IP地址等信息。

(5)证书申请者的公钥。

(6)证书颁发机构对以上信息所做的数字签名。

在进行数字签名的过程中,发送方除了向接收方发送源数据和签名的散列值外,还要发送自己的数字证书,而接收方通过发送方的数字证书获得发送方的公钥,而且接收方还可以向CA发送验证请求来验证发送方数字证书的真实性和有效性,从而确保对发送方身份验证的可靠性,带有数字证书的数字签名实现过程如图4-9所示。

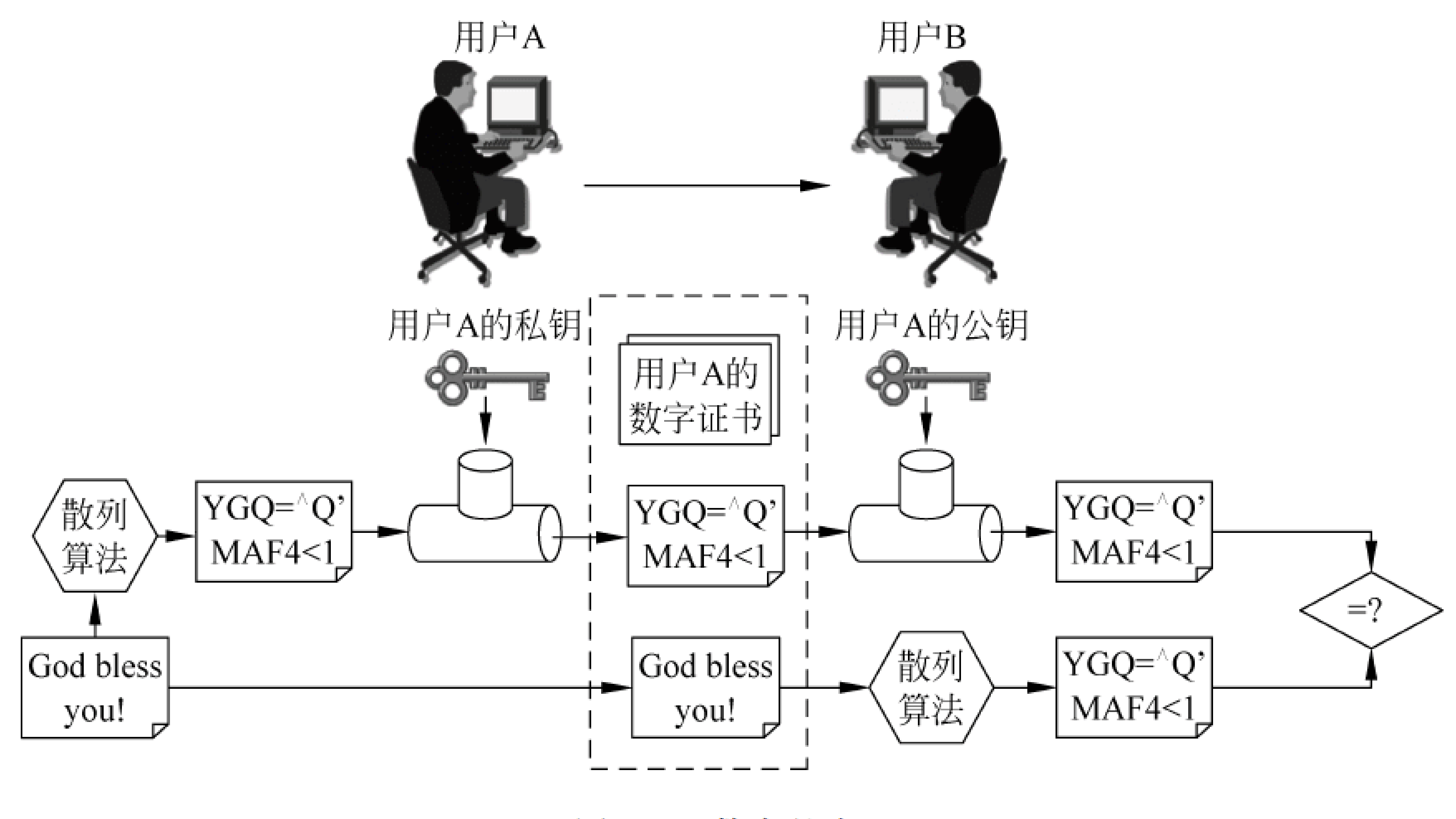


图4-9 数字签名3

要验证用户A的数字证书,接收方必须首先知道CA的公钥。通常情况下,通过带外处理或者通过安装过程中的一项操作完成。例如大多数的Web浏览器默认配置多个CA的公钥。

在通信中,身份认证通常是双向的,即发送方和接收方互相验证对端的身份。除了使用数字签名,还可以使用预共享密钥的方式进行身份认证。预共享密钥需要手工为通信双方配置相同的密钥来互相进行身份的认证。相对而言预共享密钥更加简单,但数字签名的可扩展性更好,因为预共享密钥的认证方式需要在每一对进行通信的设备之间手工配置预共享密钥,而数字签名的认证方式只要向CA申请了数字证书,通信双方自动交换数字证书,自动通过数字签名的方式即可进行身份的认证。

4.2.4 VPN拓扑

根据VPN拓扑结构的不同,可以将其分为站到站VPN和远程访问VPN两种。

1. 站到站VPN

站到站VPN又称为网络到网络(LAN-to-LAN)VPN,在站到站VPN中安全隧道两

端连接的设备功能对等，建立安全隧道时需要远端对等设备的 IP 地址。站到站 VPN 通常在两个网络的边界路由器或防火墙上配置，来保护两个特定网络之间传递数据的机密性和完整性。

2. 远程访问 VPN

远程访问 VPN 用于对远端用户，例如出差在外的员工通过公网连接到公司网络提供安全保护。远程访问 VPN 又可以分为由客户端发起和由网络接入服务器（Network Access Server，NAS）发起两种。由客户端发起的远程访问 VPN 是由远端用户使用一个 VPN 客户端或者 Web 浏览器通过公网建立到公司的安全隧道；由 NAS 发起的远程访问 VPN 是由远端用户先拨入一个 ISP NAS，然后由 NAS 建立一条去往公司网络的安全隧道，这种隧道可以支持由远端用户发起的多个会话。

4.3　站到站 VPN

在网络中存在多种技术可以建立安全隧道以实现 VPN，其中最为简单也是当前最为流行的是 IPSec（IP Security）技术。IPSec 实现于 OSI 参考模型的网络层，它在网络层定义了一个安全框架来为基于 IP 协议的上层应用提供 IPSec 隧道保护。作为一个可扩展的体系，IPSec 中可以引入多种开放的认证算法、加密算法和密钥管理体制，而不受限于任何一种特定算法。IPSec 协议簇包含了进行数据的加密、认证以及密钥交换等的一系列协议。通过这些协议和算法，IPSec 在网络中的两个端点之间提供安全的数据通信，这些端点被称为 IPSec 的对等体（Peer）。

4.3.1　IPSec 封装模式

IPSec 有两种不同的工作模式，对应两种不同的工作模式分别存在两种不同的报文封装模式，分别是隧道（Tunnel）模式和传输（Transport）模式。

1. 隧道模式

隧道模式用于在两个网络之间建立 IPSec 隧道，对等体为两个网络的边界路由器或防火墙设备。在隧道模式下，所有的加/解密和认证等均由边界路由器完成，这些操作对于进行通信的终端主机而言是完全透明的，如图 4-10 所示。

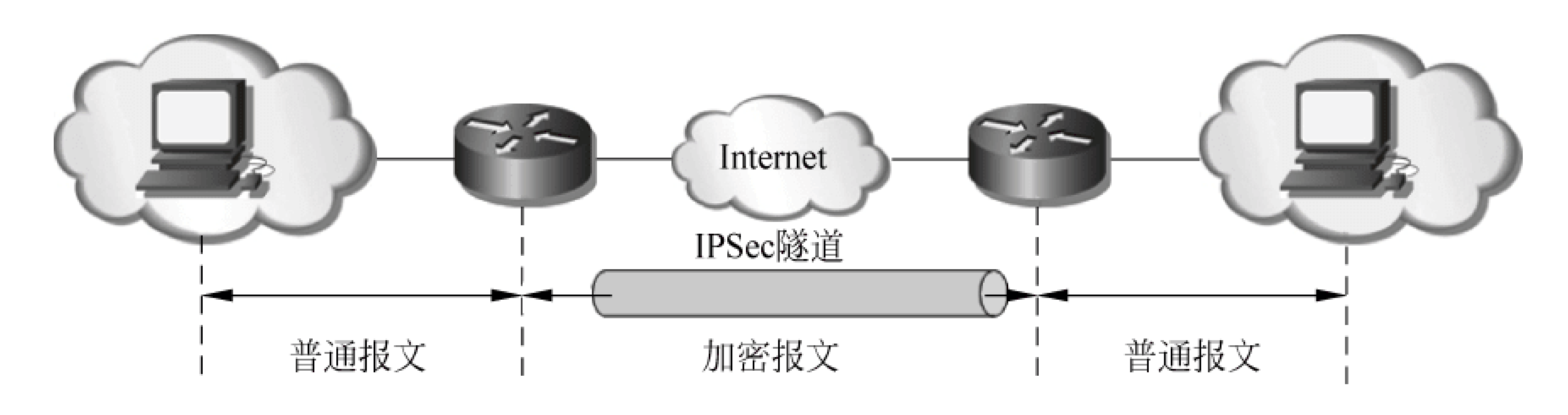


图 4-10　隧道模式

在隧道模式下，IPSec 为整个原始的 IP 报文提供安全性，用户的整个 IP 报文被加密和认证并产生 IPSec 头，然后将 IPSec 头和加密后的数据封装到一个新的 IP 报文中，新

的 IP 报头中的源 IP 地址和目的 IP 地址为两个边界路由器(即对等体)的 IP 地址,报文结构如图 4-11 所示。

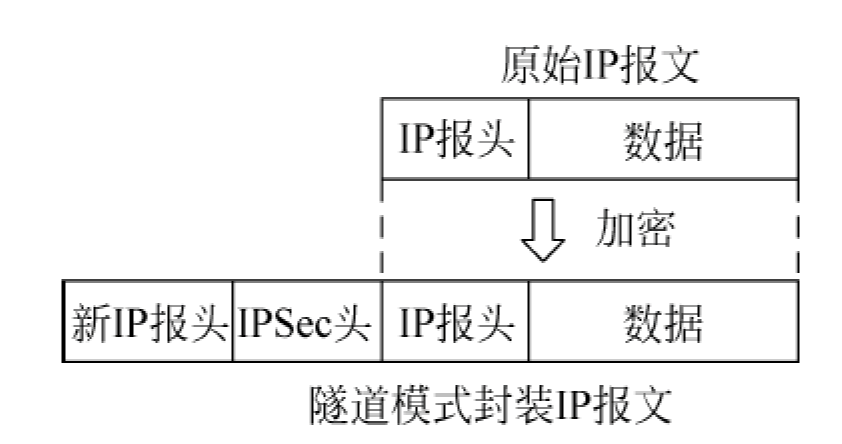


图 4-11 隧道模式报文结构

2. 传输模式

传输模式用于在两台进行通信的终端主机之间直接建立 IPSec 隧道,对等体即为进行通信的终端主机。在传输模式下,所有的加/解密和认证等均由终端主机自行完成,边界路由器仅执行正常的路由转发,不参与任何 IPSec 的过程,如图 4-12 所示。

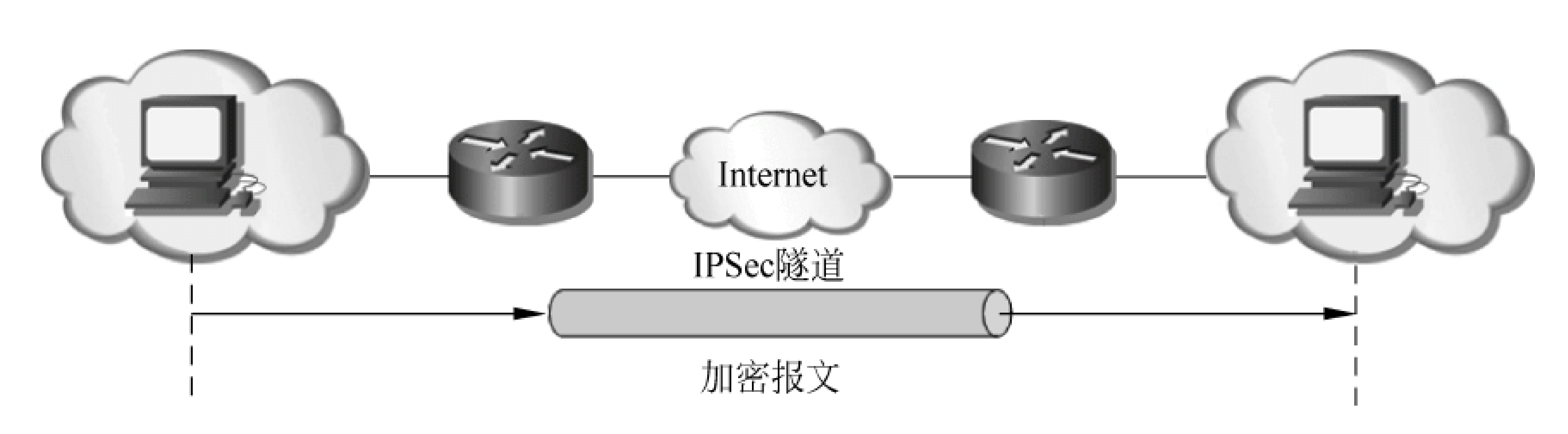


图 4-12 传输模式

在传输模式下,IPSec 只对传输层及以上层的数据提供安全性,传输层数据被加密和认证并产生 IPSec 头,将 IPSec 头插入到原始 IP 报文中 IP 报头的后面形成新的 IP 报文,而原 IP 报头保持不变,报文结构如图 4-13 所示。

两种模式相比较而言,隧道模式的安全性更好,因为隧道模式可以对整个原始 IP 报文进行认证和加密,并且使用 IPSec 对等体的 IP 地址来隐藏通信终端主机的 IP 地址。但是由于隧道模式产生了一个额外的 IP 报头,因此它会比传输模式占用更多的带宽。在实际应用中,只有在需要端到端的安全性的时候才会使用传输模式,否则一般都会使用隧道模式,而且在一些低端的路由器上只支持隧道模式,而不支持传输模式。

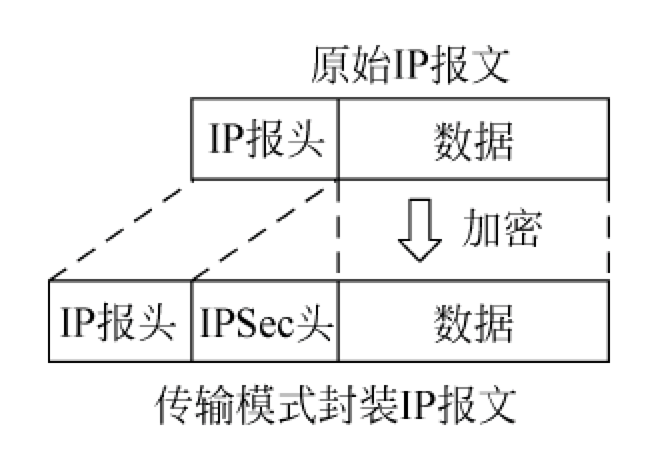


图 4-13 传输模式报文结构

4.3.2 IPSec 封装协议

IPSec 有两种不同的安全封装协议,分别是认证头(Authentication Header,AH)协议和封装安全载荷(Encapsulating Security Payload,ESP)协议。

1. AH 协议

AH 协议通过散列算法来提供数据源认证、数据完整性校验和防报文重放的功能。

AH 协议可以保护数据在通信过程中免受篡改，但它不能提供数据加密的功能，因此 AH 协议不能保证数据的机密性。AH 协议适用于需要确保完整性的一些非机密数据的传输。AH 协议的 IP 协议号为 51。

在隧道模式下，AH 协议的验证和封装如图 4-14 所示。

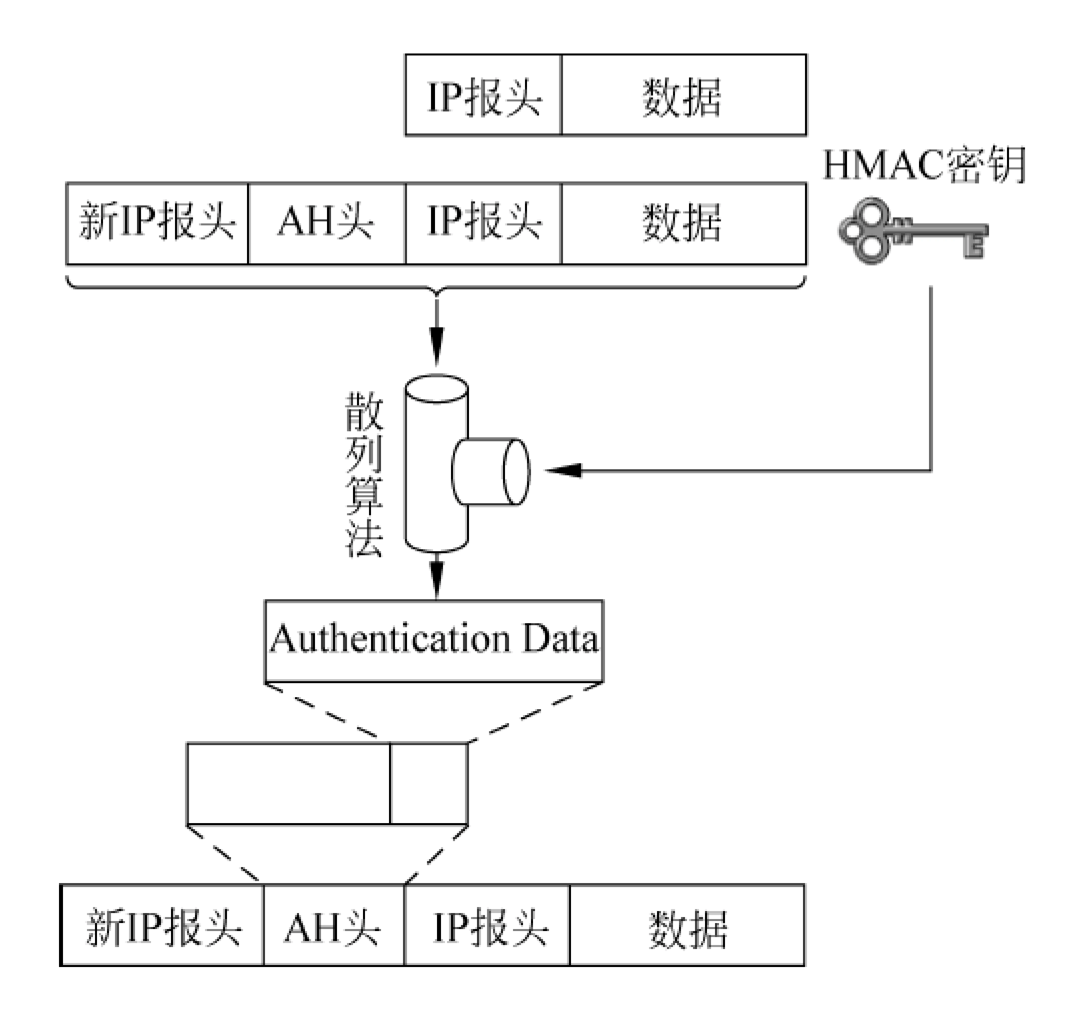


图 4-14　隧道模式下 AH 封装

从图 4-14 中可以看出，AH 协议对于整个 IP 报文的内容进行验证。在隧道模式下，经 AH 协议封装的数据报文如图 4-15 所示。

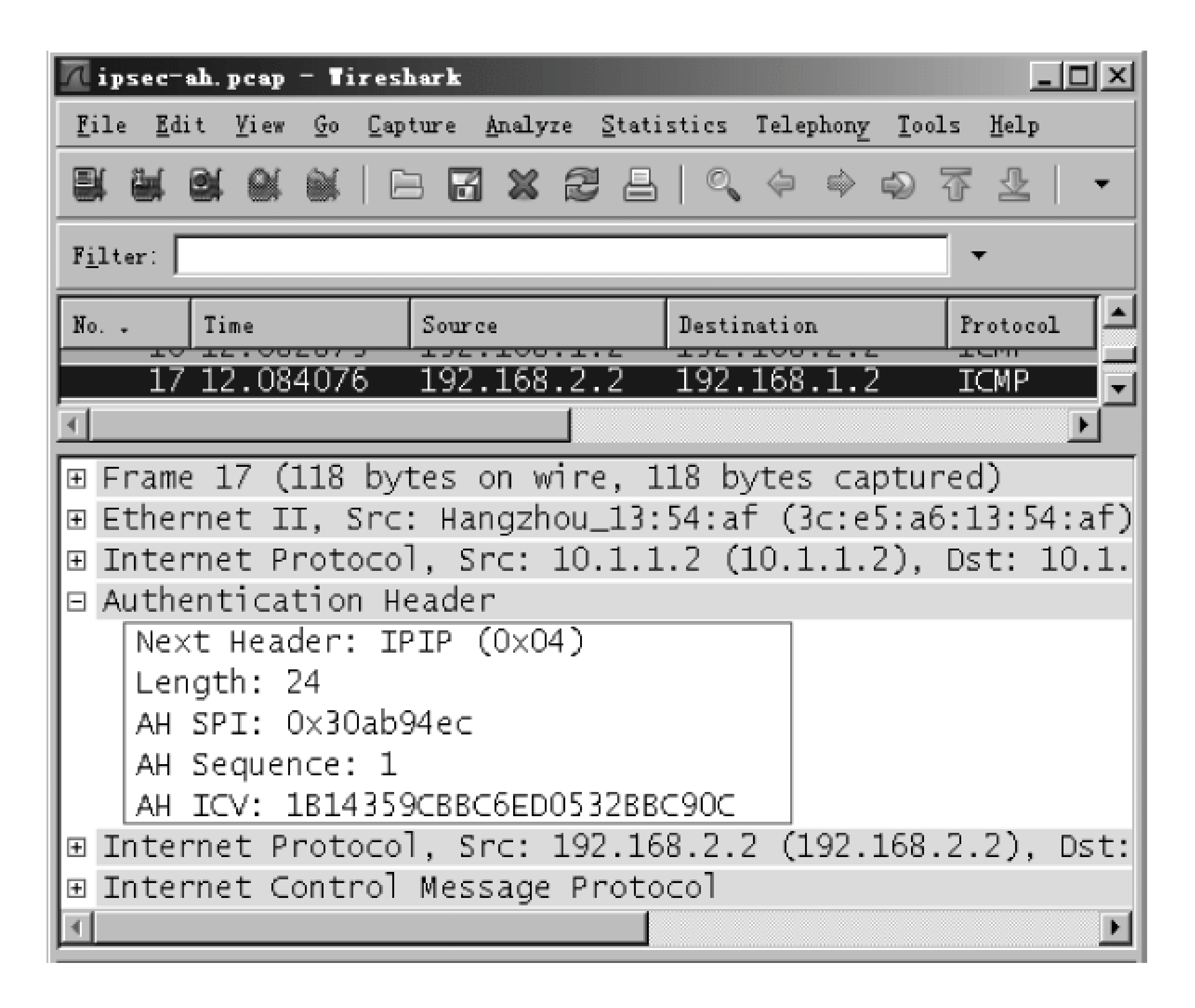


图 4-15　隧道模式下 AH 报文

从图 4-15 中可以看出，在隧道模式下 AH 协议对于报文的封装结构与图 4-13 所示相符合，报文从内向外依次是原始 IP 报文—AH 头—新 IP 报头。在 AH 头中包含了 5 个字段，分别解释如下。

(1) Next Header：下一报头协议号，用于指定 AH 协议封装中的数据报文的协议类

型,在隧道模式中总是IP协议,而在传输模式中则可能会是TCP、UDP协议等。

(2) Length:AH报头的长度,以32bit为单位。

(3) AH SPI:AH的安全参数索引(Security Parameter Index),长度为32bit,用来唯一地标识一个安全关联(Security Association,SA)。

(4) AH Sequence:从1开始的单增序列号,用来防范重放攻击。

(5) AH ICV:AH的完整性校验值(Integrity Check Value,ICV),存放的是AH通过散列算法得出的验证数据(Authentication Data)。在对整个IP报文做散列计算时,AH ICV取值为0,最后再将计算出的散列结果放置到该字段。

实际上在AH头中还存在一个16bit的保留字段,该字段处于Length字段之后,取值为0。

使用AH协议进行封装时,可选的认证算法有HMAC-MD5和HMAC-SHA1。

2. ESP协议

ESP协议通过对称加密算法和散列算法来提供加密、数据源认证、数据完整性校验和防报文重放的功能。ESP协议适用于需要确保机密性的数据传输。ESP协议的IP协议号为50。

在隧道模式下,ESP协议的验证和封装如图4-16所示。

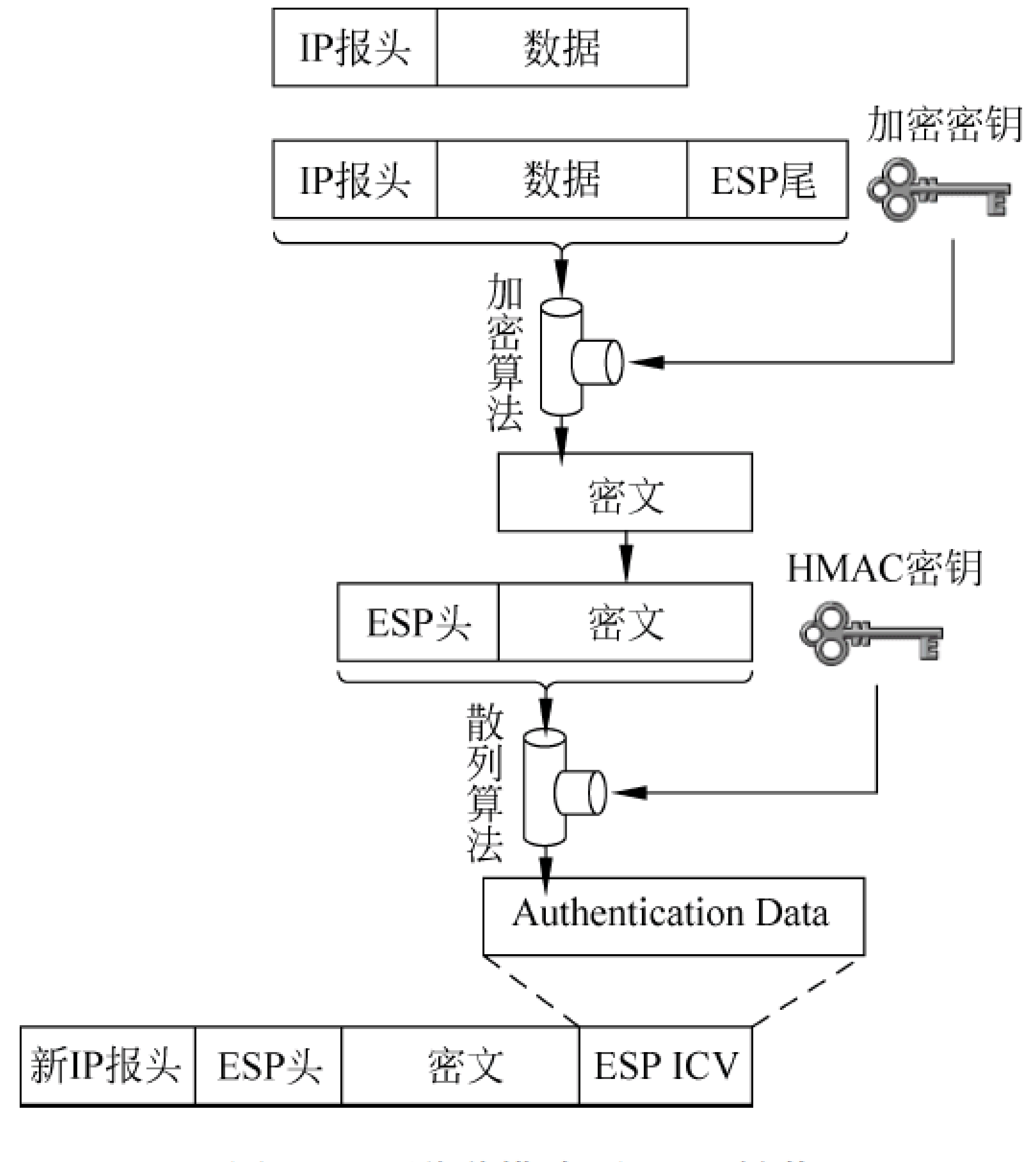


图4-16 隧道模式下ESP封装

从图4-16中可以看出,ESP协议先对数据进行加密,然后进行验证。与AH协议不同的是,ESP协议只对ESP封装部分进行了完整性的验证,并没有对新的IP报头的内容进行验证;而AH协议则对整个IP报文的内容进行了完整性验证。另外,ESP封装除了增加一个ESP头外,还在报文后面增加了一个ESP尾。在ESP提供加密服务时,原始IP报文和ESP尾均以密文的形式出现。在隧道模式下,经ESP协议封装的数据报文如图4-17所示。

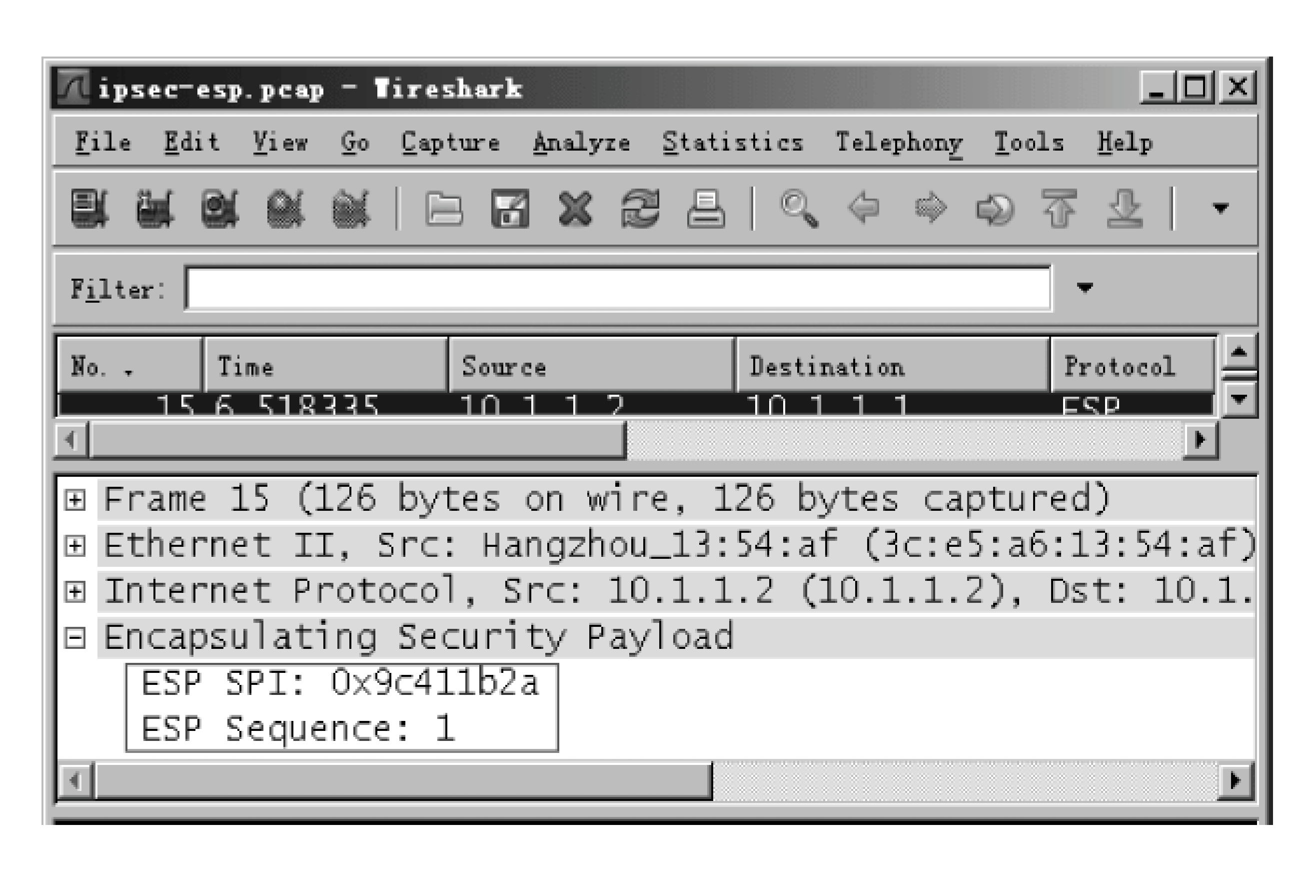


图 4-17　隧道模式下 ESP 报文

从上图中可以看出,在隧道模式下经由 ESP 协议封装的报文仅能够看到 ESP SPI 和 ESP Sequence 两个字段的内容,其他内容均为密文。

使用 ESP 协议进行封装时,可选的加密算法有 DES、3DES 和 AES,可选的认证算法有 HMAC-MD5 和 HMAC-SHA1。

ESP 协议和 AH 协议相比较而言,优点是可以提供数据的加密,但 ESP 协议的数据验证功能相对较弱。因此在实际网络通信中可以选择单独使用其中的一种协议,也可以选择同时使用这两种协议。在同时使用 AH 协议和 ESP 协议时,IPSec 会首先对报文进行 ESP 的封装,然后再对报文进行 AH 的封装,封装之后的报文从内向外依次是原始 IP 报文—ESP 头—AH 头—新 IP 报头,如图 4-18 所示。

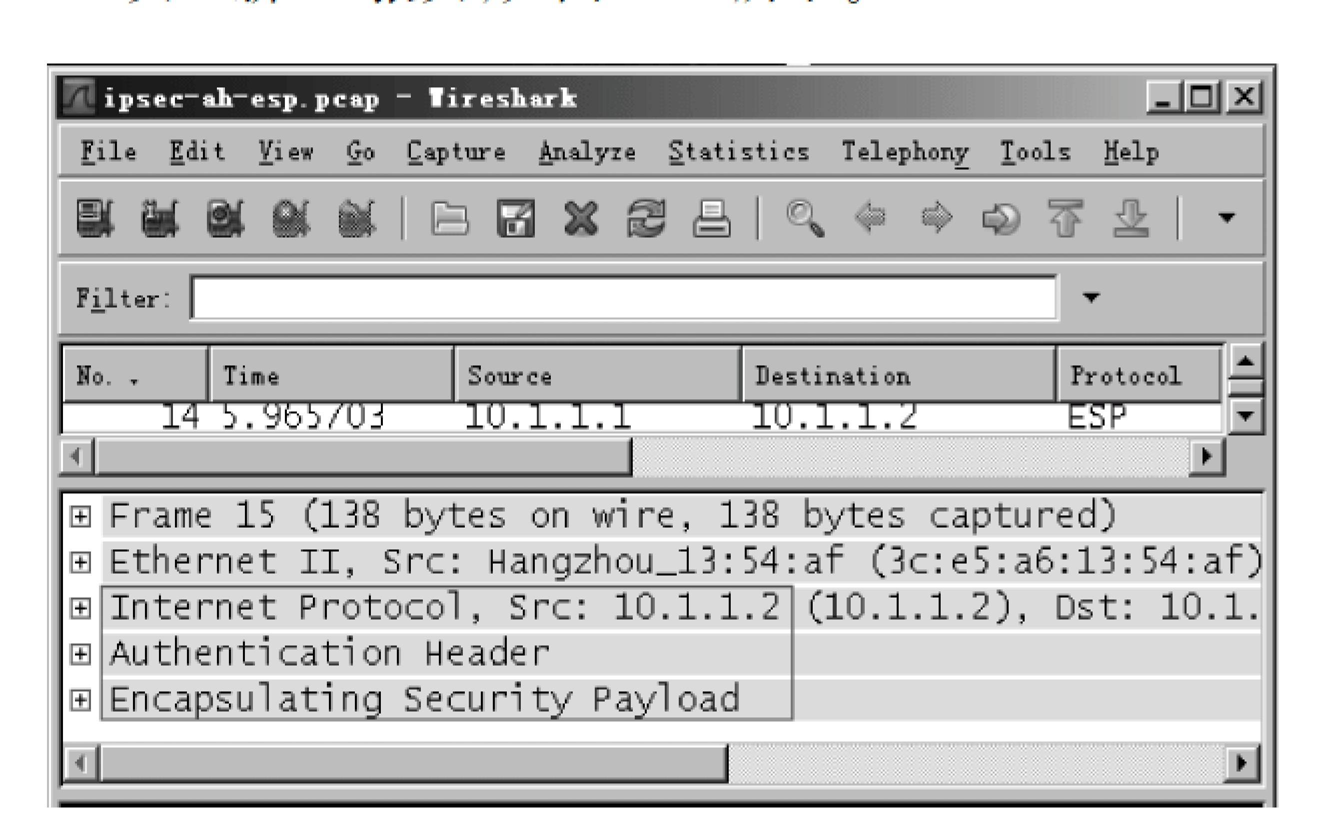


图 4-18　隧道模式下 AH-ESP 报文

4.3.3　IPSec 安全关联

安全关联(Security Association,SA)是通信双方就如何保证通信安全达成的一个协定,它描述了对等体将如何使用 IPSec 安全服务来保护网络流量,包括使用 ESP 还是 AH 协议进行数据封装、封装模式是隧道模式还是传输模式、使用哪一种加密算法、使用哪一种散列算法等。在进行安全通信之前,首先必须要在对等体之间建立 SA。

SA是单向的，一个SA就是两个对等体之间的一个单向逻辑连接，在两个对等体之间的双向通信，需要两个SA来分别对两个方向上的数据流进行安全保护。另外，SA还是协议相关的，AH协议和ESP协议都需要建立自己单独的SA。如果两个对等体之间同时使用AH协议和ESP协议进行安全通信，则需要建立4个SA来分别对两个协议的两个方向上的数据流进行安全保护。

SA由一个三元组(SPI，目的IP地址，安全协议标识符)来做唯一的标识。其中SPI是一个32bit的数值，用来唯一标识一个SA，在4.2.2节中已经作过介绍；目的IP地址即为对端对等体的IP地址；安全协议标识符是指封装协议AH或ESP。

在IPSec设备中，存在安全策略数据库(Security Policy Database，SPD)和安全关联数据库(Security Association Database，SAD)。在SPD中存储着设备上已经配置了的安全策略，安全策略的内容包括对哪些数据提供安全服务，提供的安全服务使用的封装协议、封装模式、加密算法、散列算法等。在SAD中存储着设备上处于活跃状态的所有SA。在IPSec设备上，对于出站数据报文首先将其与SPD中的安全策略相比较，如果匹配了其中的一项安全策略，则系统就会使用该项安全策略在SAD中对应的SA对数据报文进行加密认证等处理，如果在SAD中不存在相对应的SA，则需要首先建立一个SA。

SA可以通过手工配置和自动协商两种方式建立。手工配置方式需要用户在通信的对等体两端配置创建SA所需的全部信息，配置相对比较复杂，而且无法支持一些例如定时更新密钥等的高级特性。自动协商方式由互联网密钥交换(Internet Key Exchange，IKE)协议基于对等体的SPD自动协商建立和维护SA，不需要用户的干预，配置相对比较简单。在手工配置SA时，需要手工指定SPI的取值，而在IKE协商建立SA时，SPI将随机生成。在进行通信的对等体设备数量较少时，或是在小型静态环境中，可以采用手工配置方式建立SA；而在大中型的动态网络环境中，建议使用IKE协商建立SA。另外，在Web界面配置IPSec VPN时，只支持采用IKE自动协商方式建立SA。

4.3.4 IKE协议

IKE协议是一个混合型协议，它采用了互联网安全关联和密钥管理协议(Internet Security Association and Key Management Protocol，ISAKMP)所定义的密钥交换框架体系，工作于UDP的500端口上。IKE为IPSec提供了对等体身份认证、自动协商交换密钥以及建立IPSec SA的服务，简化了IPSec的配置和维护管理工作。

IKE具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥并建立IPSec SA。IKE定义了一个两阶段的工作模型，通过两个阶段为IPSec协商并建立SA。

1. 建立ISAKMP SA

在第一个阶段，首先在对等体之间经协商建立起一个通过身份认证和安全保护的通道，即建立一个ISAKMP SA，来为第二个阶段的协商提供安全服务。第一个阶段协商的主要内容包括：第一阶段使用的加密和散列算法；使用D-H算法生成并交换会话密钥资料；对等体的身份认证等。第一阶段的协商有主模式(Main Mode)和野蛮模式(Aggressive Mode)两种。

主模式使用 6 条消息协商并建立 ISAKMP SA。这 6 条消息分成 3 对，具体协商内容如下。

（1）第一对消息称为 SA 交换消息，用来协商确认第一阶段的安全策略。协商的内容包括散列算法、加密算法、身份认证方式、D-H 组和 SA 的生存周期等 5 个元素。

（2）第二对消息称为密钥交换消息，用来交换 D-H 的公开参数和辅助数据，并由对等体分别独立计算出共同的秘密 K。后续所有的加密和散列使用的密钥都由 K 衍生而来。

（3）第三对消息是 ID 信息和认证数据交换信息，对等体互相进行身份认证并对整个第一阶段交换的内容进行认证。

主模式的协商过程如图 4-19 所示。

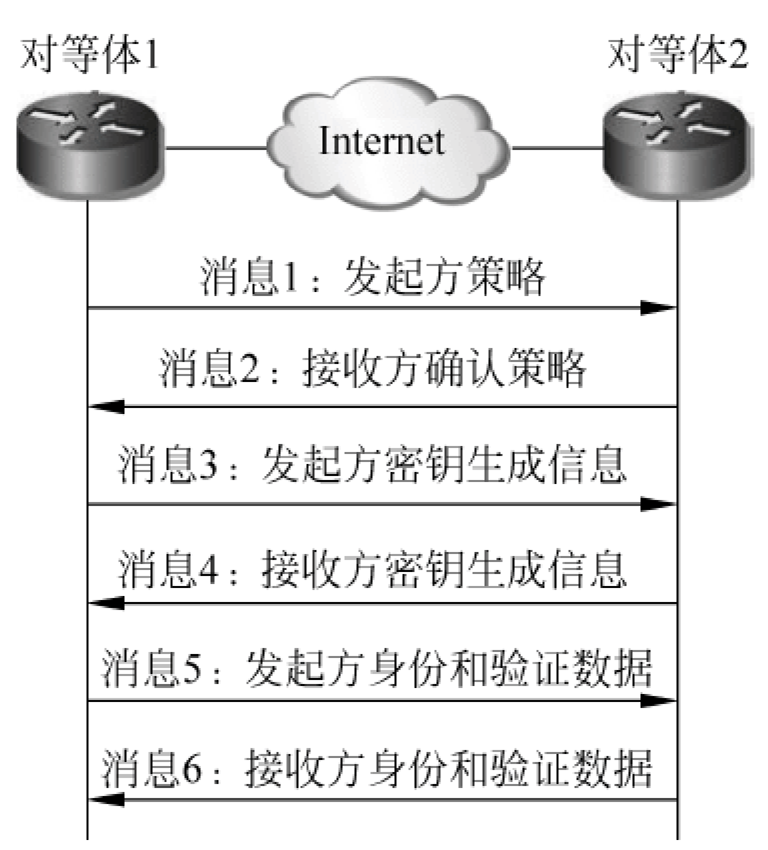


图 4-19　主模式协商过程

野蛮模式只交换 3 条信息来进行第一阶段的协商，因此野蛮模式可以提高协商的速度，但是野蛮模式不能提供对对等体身份的保护，一般用于对身份保护要求不高的场合。

2. 建立 IPSec SA

在第二个阶段，使用在第一个阶段建立的安全通道交换信息，协商建立用于传输 IP 业务数据的安全通道 IPSec SA。第二个阶段的协商只有一种模式，称为快速模式（Quick Mode）。在快速模式下使用 3 条信息协商并建立 IPSec SA。第二个阶段协商的主要内容包括：使用的 IPSec 封装协议，相应封装协议使用的散列算法和加密算法，需要保护的网络流量，IPSec 封装模式，密钥生存周期等信息。

3. IPSec 与 IKE 的关系

IPSec 和 IKE 的关系如图 4-20 所示。

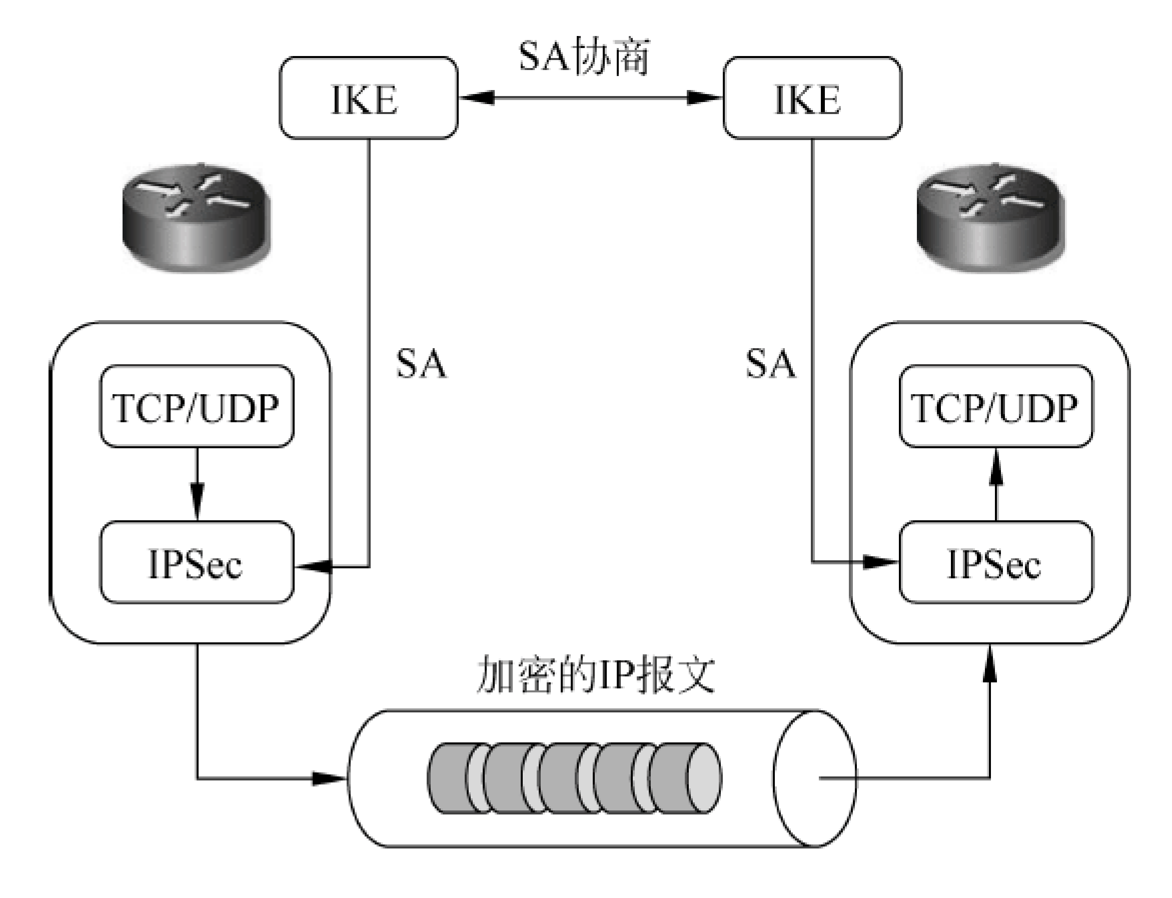


图 4-20　IPSec 与 IKE 的关系

IPSec实现于网络层,而IKE是工作于UDP协议之上的一个应用层协议,IKE是IPSec的信令协议;IKE为IPSec协商建立SA,并把建立的参数以及生成的密钥交给IPSec;IPSec使用IKE建立的SA为IP报文进行加密或认证处理。

4.3.5 IPSec的配置

1. H3C设备配置

IPSec的配置比较复杂,包括配置IKE提议和对等体、配置安全ACL、配置安全提议、配置安全策略以及在接口上应用安全策略组。本节只对Web界面下的配置进行介绍,对命令行下的配置感兴趣的同学可以自行查阅相关资料。

在此以H3C MSR 20-40路由器为例介绍IPSec VPN的配置。首先通过IE登录到路由器上,登录界面如图4-21所示。



图4-21 路由器登录界面

H3C设备默认的用户名和密码均为admin,输入用户名、密码和验证码后单击“登录”按钮进入路由器的管理平台界面。在管理平台界面左侧的导航栏中选择“VPN>IPSec VPN”,进入“IPSec连接”界面,如图4-22所示。

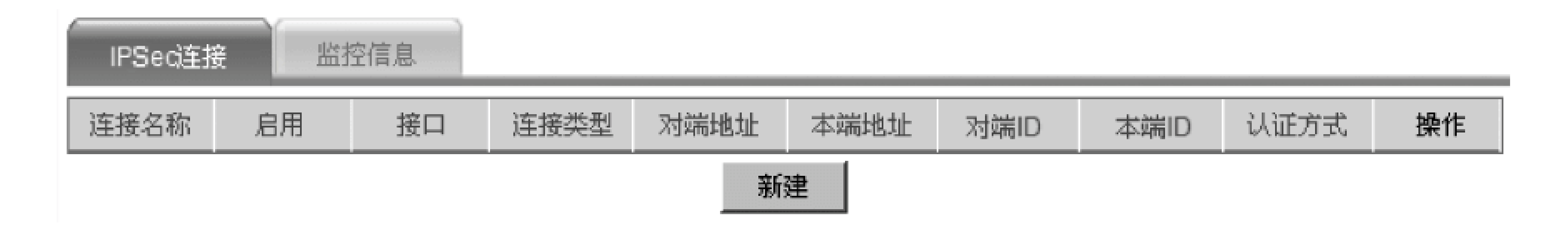


图4-22 IPSec连接界面

在“IPSec连接”界面下单击“新建”按钮进入新建IPSec连接的界面,如图4-23所示。

IPSec配置的参数项和具体的解释如下。

(1) IPSec连接名称:为IPSec连接设置一个名称,该名称只有本地意义,两端对等体的IPSec连接名称可以不同。

(2) 接口:设置要通过该IPSec连接加解密的数据流所在的接口。IPSec安全策略除了可以应用到串口、以太网口等实际的物理接口上以外,还能够应用到Tunnel、Virtual Template等虚接口上。

(3) 组网模式:设置IPSec连接的组网模式,包括站点到站点和PC到站点两种模式。

(4) 对端网关地址/主机名:设置IPSec连接对端安全网关的地址,可以是IP地址或

新建IPSec连接

IPSec连接名称 *字符（1–32）

网关信息

接口 Cellular0/0

组网模式 ⦿站点到站点 ○PC到站点

网关地址

对端网关地址/主机名 *字符（1–255）

本端网关地址

认证

认证方式

⦿预共享密钥 *字符（1–128）

○证书

网关ID

对端ID类型 ⦿IP地址 ○网关名称

本端ID类型 ⦿IP地址 ○网关名称

筛选器

筛选方式 流量特征

源地址/通配符 0.0.0.0 / 0.0.0.0 *

目的地址/通配符 0.0.0.0 / 0.0.0.0 *

▼高级

第一阶段

交换模式 ⦿主模式 ○野蛮模式

认证算法 SHA1

加密算法 DES

DH Diffie-Hellman Group1

SA的生存周期 86400 秒（60–604800，默认值=86400）

第二阶段

协议 ESP

ESP认证算法 MD5

ESP加密算法 3DES

封装模式 ⦿隧道模式 ○传输模式

PFS None

SA的生存周期

基于时间的生存周期 3600 秒（180–604800，默认值=3600）

基于流量的生存周期 1843200 千字节（2560–4294967295，默认值=1843200）

DPD ○开启 ⦿关闭

选择加密卡 << >>

星号（*）为必须填写项

确定 取消

图 4-23 IPSecVPN 配置界面

主机名。如果使用IP地址,则可以是一个IP地址,也可以是一个IP地址范围。如果本端为IKE协商的发起端,则此配置项所配IP地址必须唯一,并且要和响应端的配置的“本端网关地址”相同;如果本端为IKE协商的响应端,则此配置项所配的IP地址必须包含发起端的“本端网关地址”。如果使用主机名,则该主机名应能够被DNS服务器解析为IP地址,并且本端只能作为IKE协商的发起端。

(5)本端网关地址:设置本端的网关地址,默认情况下本端网关地址即为应用IPSec连接的接口IP地址。一般情况下本端网关地址不需要进行配置,除非用户需要指定特殊的IP地址(如Loopback接口的IP地址)作为本端网关地址。

(6)认证方式:设置对等体之间进行身份认证的方式。如果采用预共享密钥的方式进行认证,需要在两个对等体上手工设置相同的预共享密钥;如果采用证书的认证方式,则需要选择一个本地证书主题,本地证书在导航栏的“证书管理”中进行配置。

(7)对端ID类型:设置IKE在第一阶段的协商过程中使用的对端网关ID类型。如果选择网关名称作为对端ID,则需要指定对端网关ID。

(8)本端ID类型:设置IKE在第一阶段的协商过程中使用的本端网关ID类型。如果选择网关名称作为对端ID,则需要指定本端网关ID。在第一阶段使用主模式进行协商时,对端ID类型和本端ID类型都只能使用IP地址。

(9)筛选方式:设置筛选需要被IPSec保护的数据流方式。采用流量特征的筛选方式表示根据指定筛选条件筛选出需要IPSec保护的数据流,此时需要指定数据流的匹配条件,即源地址/通配符和目的地址/通配符;采用对端指定的筛选方式表示由对端对等体指定需要IPSec保护的数据流。筛选方式设置为对端指定的一端不能作为IKE协商的发起端。

(10)源地址/通配符和目的地址/通配符:设置需要IPSec保护的数据流筛选条件,即设置一个高级ACL,由该ACL显式permit的流量将被IPSec保护。在两端对等体上配置的筛选条件必须是完全对称的,即一端对等体上配置的源地址/通配符要和另一端对等体上配置的目的地址/通配符相同。

(11)交换模式:设置IKE第一阶段的交换模式为主模式还是野蛮模式。

(12)认证算法:设置IKE第一阶段使用的散列算法,可选择SHA1或MD5算法。

(13)加密算法:设置IKE第一阶段使用的加密算法,可选择DES、3DES、AES-128、AES-192或AES-256算法。

(14)DH:设置IKE第一阶段密钥协商时采用的D-H密钥交换参数。

(15)SA的生存周期:设置ISAKMP SA的生存周期,即主密钥的生存周期。主密钥即为D-H算法计算出的共同秘密K,在第二阶段对IP业务数据进行保护的密钥称为会话密钥,会话密钥均由主密钥衍生而来。

在设定的生存周期超时前,会提前协商新的ISAKMP SA来替换旧的SA。在新的SA还没有协商完之前,依然使用旧的SA;在新的SA建立后,将立即使用新的SA,而旧的SA在生存周期超时后被自动清除。

由于ISAKMP SA的重新协商需要对等体之间进行身份认证,并且要进行D-H交换,这可能需要相对较长的时间,因此一般ISAKMP SA的生存周期要比IPSec SA的生

存周期要长(即主密钥的生存周期要比会话密钥的生存周期长),在MSR 20-40上默认为24h。

(16) 协议:设置IPSec使用的安全封装协议,可选择ESP、AH或AH-ESP协议。

(17) ESP认证算法、ESP加密算法和AH认证算法:设置相应安全封装协议的散列和加密算法。AH认证算法可选择SHA1或MD5算法;ESP认证算法可选择SHA1、MD5算法或NULL,NULL表示不进行ESP认证;ESP加密算法可选择DES、3DES、AES-128、AES-192、AES-256算法或NULL,NULL表示不进行ESP加密。ESP认证算法和ESP加密算法不能同时设置为NULL。

(18) 封装模式:设置IPSec的封装模式是隧道模式还是传输模式。

(19) PFS:设置第二阶段的协商是否使用完善的前向安全(Perfect Forward Secrecy,PFS)特性,并指定采用的D-H组。PFS决定了密钥的生成方式,确保了密钥之间的无关性,即使攻击者破解了一个密钥,也只能获知该密钥加密的数据,而无法获知其他的加密数据。这就要求生成一个密钥的材料不能用来生成其他的密钥。第二阶段的PFS特性(即会话密钥PFS特性)通过在第二阶段的协商中进行一次附加的密钥交换来实现。

(20) SA的生存周期:设置IPSec SA的生存周期,即会话密钥的生存周期。IPSec SA的生存周期有两种定义方式:基于时间的生存周期用来定义一个IPSec SA从建立到失效的时间,默认为1h;基于流量的生存周期用来定义一个IPSec SA允许处理的最大流量,默认为1843200KB。

在设定的生存周期超时前,会提前协商新的IPSec SA来替换旧的SA。在新的SA还没有协商完之前,依然使用旧的SA;在新的SA建立后,将立即使用新的SA,而旧的SA在生存周期超时后被自动清除。实际上就是在定义的时间或流量的生存周期到期时需要更新会话密钥,会话密钥的生存周期比主密钥的生存周期要短,新的会话密钥通过主密钥加密在对等体之间进行传递,一次通信过程可能会用到多个会话密钥,对会话密钥的反复加密也可能会导致主密钥的失密。

在两端对等体配置的生存周期不同时,采用其中生存周期较小的一个。

(21) DPD:对等体死亡探测(Dead Peer Detection)功能用于对对端对等体状态进行探测,避免因对端对等体掉线而出现加密黑洞。开启DPD功能需要设置"触发DPD的时间间隔"和"等待DPD响应报文的时间"两个参数。如果在触发DPD的时间间隔中没有收到来自对端的IPSec报文,则本端触发发送DPD查询,同时计时器开始计时,如果在等待DPD响应报文的时间到时之前无法收到对端的DPD响应报文则认为对端掉线,删除ISAKMP SA和相应的IPSec SA。当有符合安全策略的报文需要发送时,会重新触发设备协商建立SA。

假设存在如图4-24所示的网络,网络联通性已经配置完成。要求配置IPSec VPN来保护192.168.1.1/24和192.168.2.0/24两个网段之间的通信流量,其中对等体身份认证采用预共享密钥的方式,预共享密钥为123456,其他配置均采用系统默认配置。

首先在交换机SWA上配置端口镜像,将端口E1/0/1和E1/0/2的出入站流量均镜像到端口E1/0/24上,具体的配置命令如下:

```
[SWA]mirroring-group 1 local
[SWA]mirroring-group 1 mirroring-port Ethernet 1/0/1 to Ethernet 1/0/2 both
[SWA]mirroring-group 1 monitor-port Ethernet 1/0/24
```

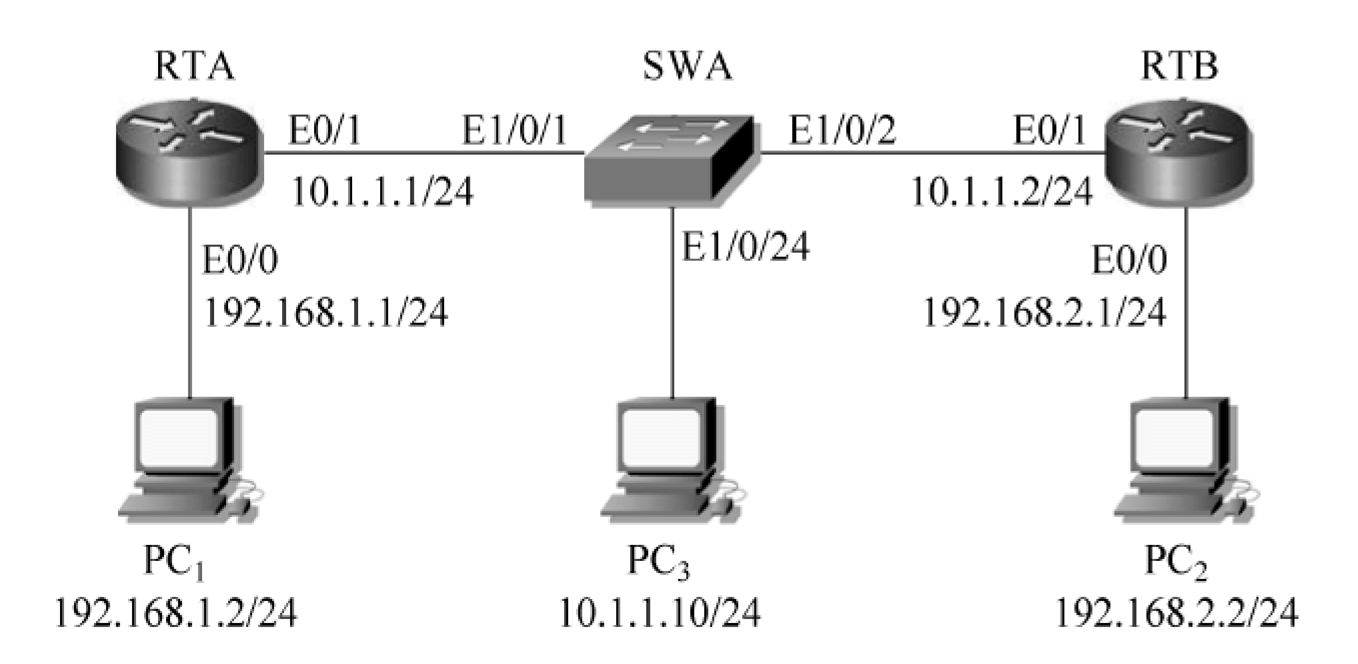


图 4-24　IPSec VPN 配置网络拓扑结构

在路由器 RTA 上配置 IPSec VPN，具体的配置如图 4-25 所示。

新建IPSec连接
IPSec连接名称　abc　*字符（1－32）
网关信息
接口　Ethernet0/1
组网模式　◉站点到站点　○PC到站点
网关地址
对端网关地址/主机名　10.1.1.2　*字符（1－255）
本端网关地址
认证
认证方式
◉预共享密钥　••••••　*字符（1－128）
○证书
网关ID
对端ID类型　◉IP地址　○网关名称
本端ID类型　◉IP地址　○网关名称
筛选器
筛选方式　流量特征
源地址/通配符　192.168.1.0　/0.0.0.255　*
目的地址/通配符　192.168.2.0　/0.0.0.255　*
▶高级
星号（*）为必须填写项
确定　取消

图 4-25　RTA 上 IPSec VPN 的配置

路由器 RTB 上的配置与 RTA 类似，区别是 RTB 上设置的对端网关地址/主机名为 10.1.1.1；筛选器中源地址/通配符为 192.168.2.0/0.0.0.255，目的地址/通配符为 192.168.1.0/0.0.0.255，与路由器 RTA 上的筛选器完全对称。

配置完成后，在 PC_1 上使用 ping 命令连接 PC_2，同时分别在 3 台 PC 上使用 Wireshark 软件捕获数据报文。在 PC_1 和 PC_2 上捕获的数据报文为 ICMP 的明文，而在 PC_3 上捕获的数据报文中，可以看到 IKE 协议进行 ISAKMP SA 和 IPSec SA 协商的数据报文，以及使用第二阶段默认的安全协议 ESP 进行封装的 PC_1 和 PC_2 之间的通信数据，具体如图 4-26 所示。

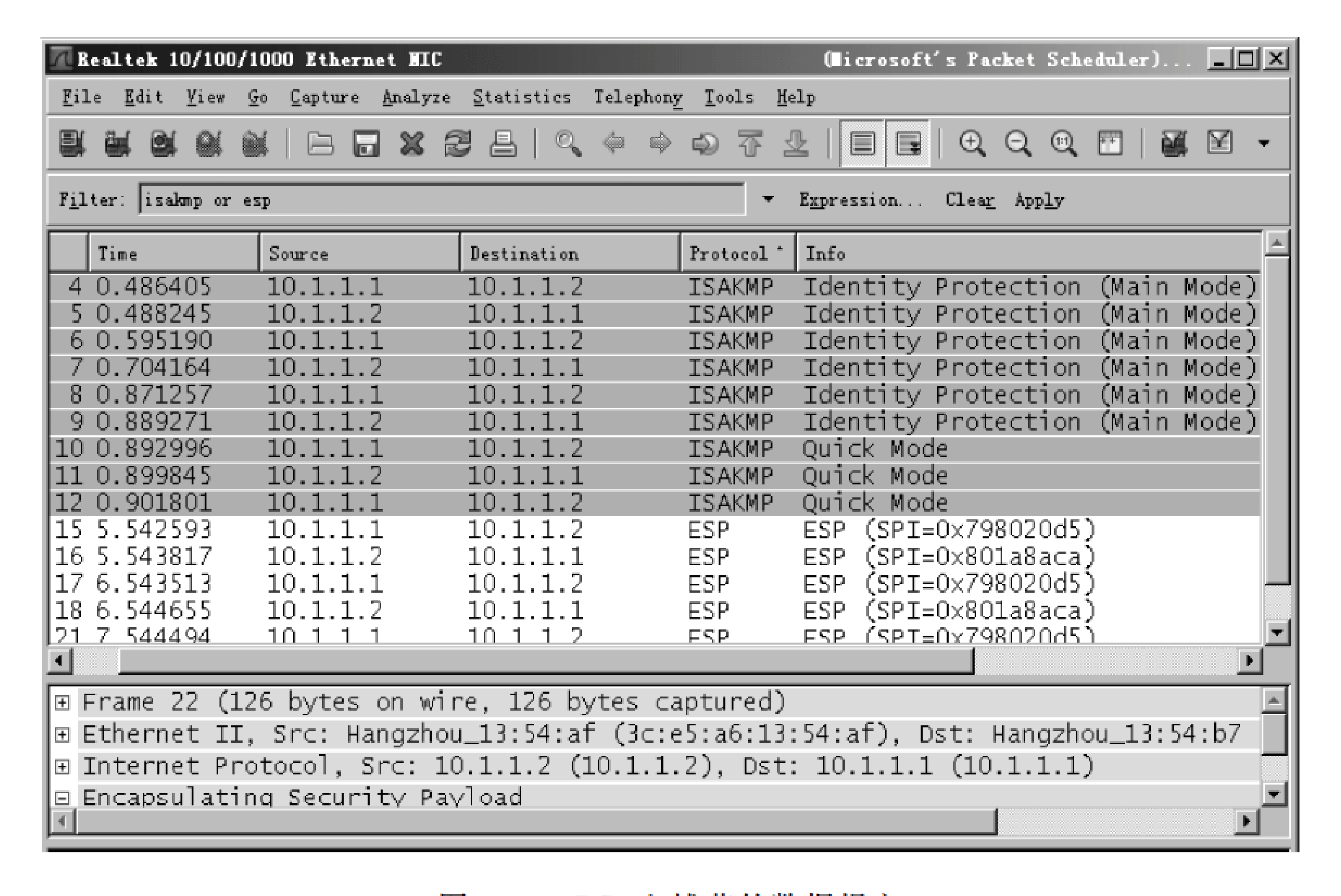


图 4-26　PC_3 上捕获的数据报文

从图 4-26 中可以看到，ESP 封装的数据报文的源 IP 地址和目的 IP 地址分别是两端对等体的 IP 地址，而不是终端主机的 IP 地址。

在路由器 RTA 或路由器 RTB 的"IPSec 连接"界面下单击"监控信息"进入监控信息界面，可以看到 IPSec 连接信息。选中某个连接信息前的复选框，可以在"隧道列表"中看到该连接下已建立的隧道信息，路由器 RTA 上的监控信息如图 4-27 所示。

IPSec连接　监控信息

	连接名	接口	对端地址	本端地址	连接状态	最近-最近一次连接错误
☑	abc	Ethernet0/1	10.1.1.2		Connected	ERROR_NONE

隧道列表

对端地址	流量特征	SPI	出/入报文数	出/入字节数	操作
10.1.1.2	src 192.168.1.0/0.0.0.255 dst 192.168.2.0/0.0.0.255 protocol IP src-port 0 dst-port 0	in 2149223114 [ESP] out 2038440149 [ESP]	3/3	192/192	

刷新　删除选中连接的所有隧道　删除ISAKMP SA

图 4-27　路由器 RTA 上 IPSec 监控信息

从图 4-27 所示的隧道列表信息中可以看出，对于 ESP 协议在 in 和 out 方向上分别有一个 SPI，即对于 ESP 协议在 in 和 out 方向上分别存在一个 IPSec SA。单击"删除

ISAKMP SA”按钮,可以删除已建立的ISAKMP SA;单击“删除选中连接的所有隧道”按钮,可以删除选中的连接下所有已建立的IPSec隧道。

2. Cisco设备配置

Cisco设备配置站到站IPSec VPN涉及的命令如下。

(1) 启用IKE功能。

```
Router(config)#crypto isakmp enable
```

默认情况下,路由器上的IKE功能处于启用状态,因此该命令可以不配置。

(2) 创建IKE策略,即定义第一阶段ISAKMP SA协商所需的各项参数。

```
Router(config)#crypto isakmp policy priority
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption {des|3des|aes}
Router(config-isakmp)#group {1|2|5}
Router(config-isakmp)#hash {md5|sha}
Router(config-isakmp)#lifetime lifetime
```

其中,IKE策略优先级取值范围为1~10000,1的优先级最高,在进行IKE策略定义时,优先级通常从10开始创建,以备以后插入更高优先级的策略。

在IKE策略中,定义了对等体的身份认证方式为预共享密钥,同时定义了第一阶段协商使用的加密算法、散列算法、D-H算法以及ISAKMP SA的生存周期。

(3) 配置预共享密钥。

```
Router(config)#crypto isakmp key encrypt-level key-string address peer-address
```

其中,参数*encrypt-level*为密钥的加密级别,取值为0或6。必须保证对等体两端使用相同的预共享密钥,否则身份认证将会失败。

(4) 配置变换集,即定义第二阶段IPSec SA协商所需的各项参数。

```
Router(config)#crypto ipsec transform-set transform-set-name
{ah-md5-hmac|ah-sha-hmac|esp-des|esp-3des|esp-aes|esp-md5-hmac|esp-sha-hmac}
```

(5) 配置IPSec SA的生存周期。

```
Router(config)#crypto ipsec security-association lifetime {seconds seconds|kilobytes kilobytes}
```

与H3C设备上的配置类似,对IPSec SA生存周期的配置可以采用基于时间和基于流量两种方式。

(6) 配置ACL来定义受到VPN保护的流量。

```
Router(config)#ip access-list extended name
Router(config-ext-nacl)#{permit|deny} protocol source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]]
```

注意: 要保证对等体两端的ACL配置完全对称。

(7) 配置加密图。

```
Router(config)#crypto map map-name seq-number ipsec-isakmp
Router(config-crypto-map)#set peer peer-adress
Router(config-crypto-map)#set transform-set transform-set-name
Router(config-crypto-map)#match address acl-name
```

(8) 将加密图应用到接口上。

```
Router(config-if)#crypto map map-name
```

在此依然使用图 4-24 所示的网络进行 IPSec VPN 的配置，首先在交换机 SWA 上配置端口镜像，具体的配置命令如下：

```
SWA(config)#monitor session 1 source interface FastEthernet 0/1-2 both
SWA(config)#monitor session 1 destination interface FastEthernet 0/24
```

在路由器 RTA 上配置 IPSec VPN，具体的配置命令如下：

```
RTA(config)#crypto isakmp policy 10
RTA(config-isakmp)#authentication pre-share
RTA(config-isakmp)#encryption des
RTA(config-isakmp)#group 1
RTA(config-isakmp)#hash md5
RTA(config-isakmp)#lifetime 3600
RTA(config-isakmp)#exit
RTA(config)#crypto isakmp key 0 123456 address 10.1.1.2
RTA(config)#crypto ipsec transform-set ts-vpn esp-3des esp-md5-hmac
RTA(cfg-crypto-trans)#exit
RTA(config)#ip access-list extended eacl-vpn
RTA(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
RTA(config-ext-nacl)#exit
RTA(config)#crypto map map-vpn 10 ipsec-isakmp
RTA(config-crypto-map)#set peer 10.1.1.2
RTA(config-crypto-map)#set transform-set ts-vpn
RTA(config-crypto-map)#match address eacl-vpn
RTA(config-crypto-map)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#crypto map map-vpn
```

配置完成后，在路由器 RTA 上执行 show crypto isakmp policy 命令查看 IKE 策略，显示结果如下：

```
RTA#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                3600 seconds, no volume limit
Default protection suite
```

```
          encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
          hash algorithm:          Secure Hash Standard
          authentication method:  Rivest-Shamir-Adleman Signature
          Diffie-Hellman group:   #1 (768 bit)
          lifetime:               86400 seconds, no volume limit
```

执行 show crypto ipsec transform-set 命令查看变换集,显示结果如下:

```
RTA#show crypto ipsec transform-set
Transform set ts-vpn: { esp-3des esp-md5-hmac   }
   will negotiate = { Tunnel,   }
```

执行 show crypto map 命令查看加密图信息,显示结果如下:

```
RTA#show crypto map
Crypto Map "map-vpn" 10 ipsec-isakmp
          Peer = 10.1.1.2
          Extended IP access list eacl-vpn
              access-list eacl-vpn permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
          Current peer: 10.1.1.2
          Security association lifetime: 4608000 kilobytes/3600 seconds
          PFS (Y/N): N
          Transform sets={
                  ts-vpn,
          }
          Interfaces using crypto map map-vpn:
                  FastEthernet0/1
```

路由器 RTB 上的配置与 RTA 上类似,唯一的区别是访问控制列表与 RTA 上完全对称。在此不再赘述。

配置完成后的测试过程与 H3C 设备类似。

测试完毕后,在路由器 RTA 上执行 show crypto isakmp sa 查看 isakmp 的安全关联,显示结果如下:

```
RTA#show crypto isakmp sa
dst             src             state           conn-id     slot status
10.1.1.2        10.1.1.1        QM_IDLE              1         0 ACTIVE
```

在路由器 RTA 上执行 show crypto ipsec sa 命令查看 IPSec 的安全关联,显示结果如下:

```
RTA#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: map-vpn, local addr 10.1.1.1

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 10.1.1.2 port 500
```

```
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0xB0628A83(2959248003)

inbound esp sas:
  spi: 0xF60D98FE(4128086270)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 3001, flow_id: FPGA:1, crypto map: map-vpn
    sa timing: remaining key lifetime (k/sec): (4485350/2656)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB0628A83(2959248003)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 3002, flow_id: FPGA:2, crypto map: map-vpn
    sa timing: remaining key lifetime (k/sec): (4485350/2655)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

4.4 远程访问 VPN

4.4.1 L2TP VPN

作为网络层的隧道协议，IPSec 只支持 IP 单播流量，而无法对多协议或 IP 多播流量提供安全保护；在进行 IPSec 配置时，必须要配置对端网关地址(见图 4-23)，而用户出差在外地通过公网连接公司网络时其 IP 地址并不固定。因此 IPSec 一般用于配置站到站的 VPN，而要求多协议支持的远程访问 VPN 一般采用 L2TP 协议来实现。

二层隧道协议(Layer 2 Tunneling Protocol,L2TP)由IETF起草,结合了Cisco公司的二层转发(Layer 2 Forwarding,L2F)协议和Microsoft公司的点到点隧道协议(Point-to-Point Tunneling Protocol,PPTP)的优点,在数据链路层为数据提供隧道封装。L2TP通过为远程用户分配企业内部地址为企业驻外机构和出差人员提供从远程经由公共网络安全访问公司内部网络的虚拟专用拨号网(Virtual Private Dial-up Network,VPDN)。

1. L2TP基础

L2TP协议基于广域网链路上的点到点协议(Point-to-Point Protocol,PPP)实现。PPP协议通过在数据链路层上的封装,可以在点到点链路上传输多种上层协议的数据报文。而L2TP通过对PPP模型的扩展,使PPP会话可以跨越Internet网络,为远程用户和公司网络的边界路由器之间提供PPP会话。典型的L2TP组网应用如图4-28所示。

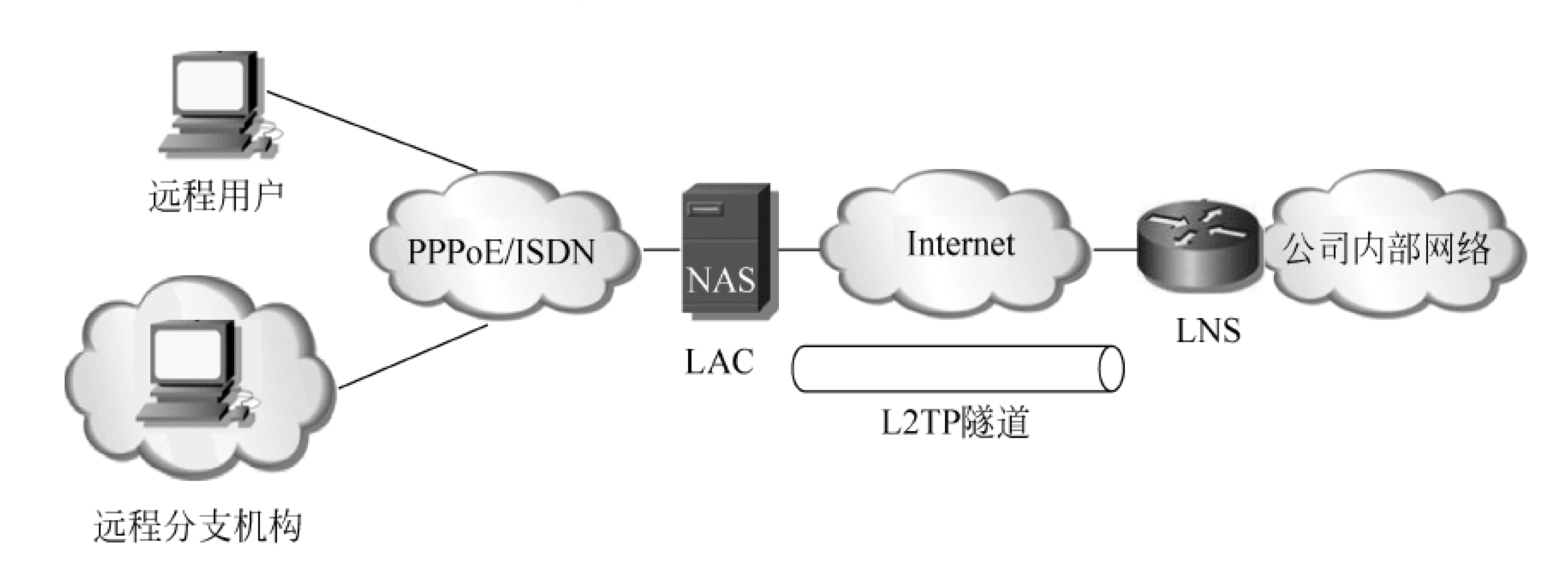


图4-28 L2TP典型组网应用

从图4-28中可以看出,L2TP组建的VPDN中,网络组件包括以下3部分。

(1) 远端系统

远端系统是需要接入到VPDN中的远程用户和远程分支机构,通常是一台通过ADSL等方式连接网络的主机或私有网络的一台路由设备。

(2) L2TP访问集中器

L2TP访问集中器(L2TP Access Concentrator,LAC)是附属在交换网络上的具有PPP端系统和L2TP协议处理能力的设备,通常是一个当地ISP的网络接入服务器(Network Access Server,NAS),主要用于为PPP类型的用户提供接入服务。

LAC位于LNS和远端系统之间,用于在LNS和远端系统之间传递数据报文。LAC将从远端系统收到的数据报文按照L2TP协议进行封装并发送给LNS,同时将从LNS收到的数据报文进行解封装并发送给远端系统。

LAC与远端系统之间采用本地连接或PPP链路,VPDN应用中通常为PPP链路。

(3) L2TP网络服务器

L2TP网络服务器(L2TP Network Server,LNS)通常是一个公司网络的边界路由器,它既是PPP端系统,又是L2TP协议的服务器端。LNS作为L2TP隧道的另一侧端点,是LAC的对端设备,是LAC进行隧道传输的PPP会话的逻辑终止端点。通过在公共网络中建立L2TP隧道,将远端系统的PPP连接的另一端由原来的LAC在逻辑上延伸到了LNS,使二层链路端点(LAC)和PPP会话点(LNS)可以驻留在通过分组交换网络

连接的不同设备上，从而扩展了 PPP 模型，使 PPP 会话可以跨越帧中继或 Internet 等网络。

2. L2TP 协议报文结构

L2TP 协议的报文封装结构如图 4-29 所示。

IP 报头（公网地址）	UDP 头	L2TP 头	PPP 头	IP 报头（私有地址）	数据

图 4-29　L2TP 协议报文结构

在 L2TP 协议中，LNS 端会为远程用户分配企业内部网络的私有 IP 地址，远程用户在访问企业内部网络时使用私有 IP 地址（相当于远程用户在逻辑上依然处于企业内部网络中），因此原始 IP 数据报文的 IP 报头中使用的为私有 IP 地址。原始 IP 数据报文依次被 PPP 协议和 L2TP 协议封装，L2TP 协议在传输层使用 UDP 协议进行封装，它使用 UDP 的 1701 端口进行通信，最外层封装上新的 IP 报头，其中的源 IP 地址和目的 IP 地址分别为远程用户的公网 IP 地址和企业边界路由器接口的 IP 地址（或 PPP Server 地址）。经 L2TP 协议封装的数据报文如图 4-30 所示。

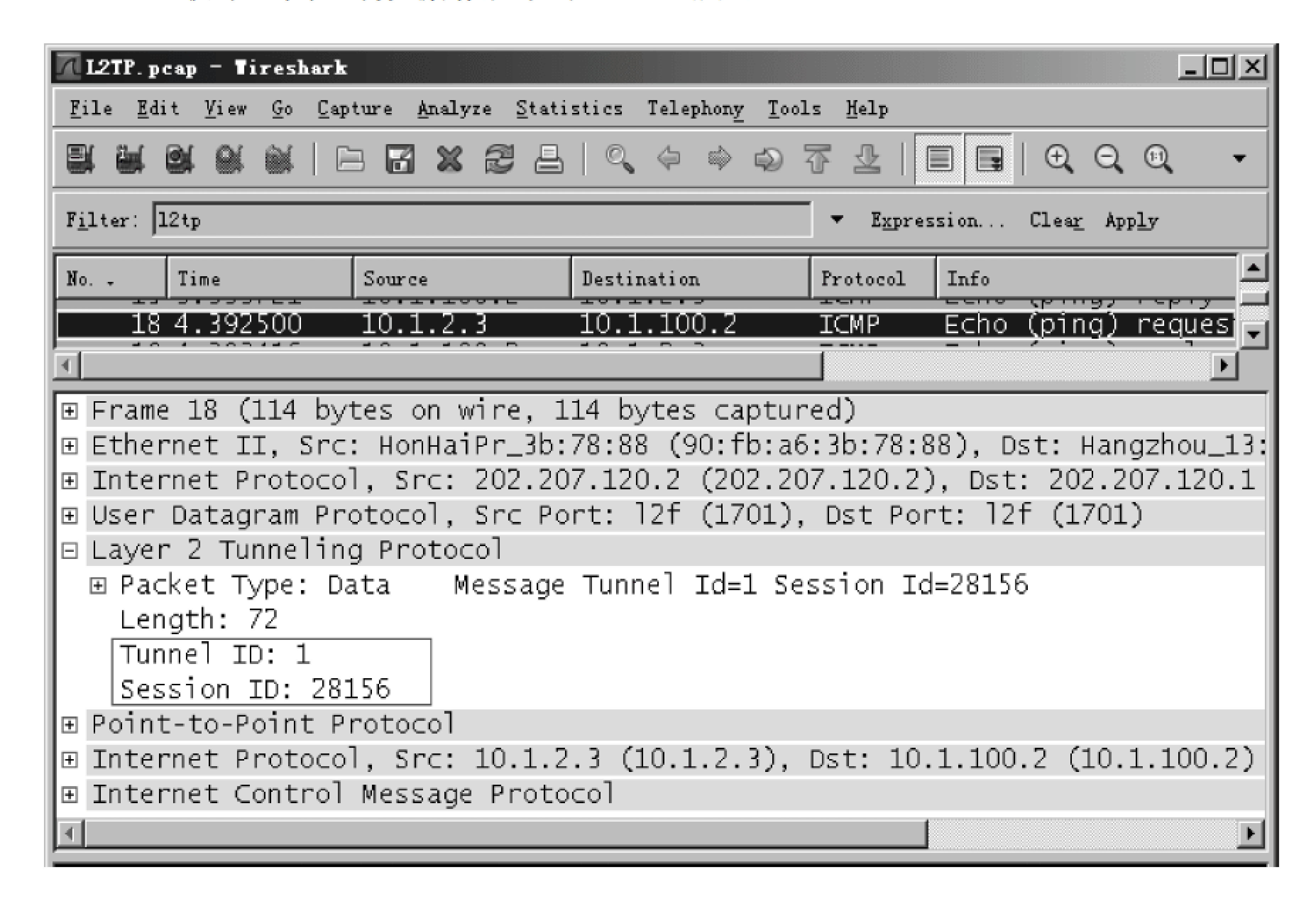


图 4-30　L2TP 协议封装的数据报文

在一个 LAC 和 LNS 之间存在着两种类型的连接：隧道（Tunnel）连接和会话（Session）连接。一个隧道连接对应了一个 LAC 和 LNS 对；而会话连接复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，一个隧道由一个控制连接和一个或多个会话连接组成。会话连接必须在隧道建立成功之后进行，每一个会话连接都对应于 LAC 和 LNS 之间的一个 PPP 数据流。

在L2TP中存在两种消息类型：控制消息和数据消息。控制消息用于隧道和会话连接的建立、维护以及传输控制，控制消息的传输是可靠的，它支持流量控制和拥塞控制；数据消息用于封装PPP数据帧并在隧道上传输，数据消息的传输是不可靠的。无论是控制消息还是数据消息都使用相同的L2TP协议报头，在L2TP报头中包含有隧道标识符(Tunnel ID)和会话标识符(Session ID)信息，如图4-29所示，用来标识不同的隧道和会话。隧道标识符相同但会话标识符不同的数据报文将被复用在同一个隧道上。

L2TP协议使用Hello报文来检测隧道的联通性，LAC和LNS定时向对端发送Hello报文，如果在一段时间内没有收到Hello报文的应答，则相应的隧道会断开。

3. L2TP隧道模式

L2TP隧道的建立包括两种模式，分别是NAS发起模式和客户端发起模式。

(1) NAS发起模式

在NAS发起模式(NAS-Initiated)中，由LAC端发起L2TP隧道连接，如图4-31所示。

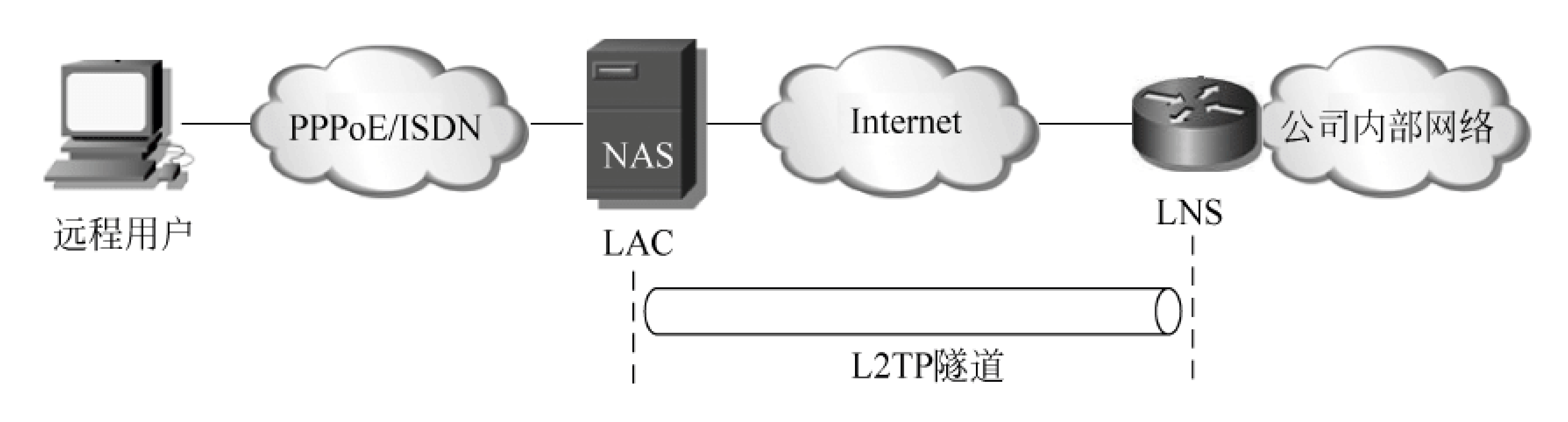


图4-31 NAS-Initiated模式

远程用户通过PPPoE/ISDN等方式拨入LAC，由LAC通过Internet向LNS发起建立隧道连接的请求，并最终在LAC和LNS之间建立L2TP隧道。对远程用户的认证、授权和计费等可由LAC侧的代理完成，也可以在LNS侧完成。

(2) 客户端发起模式

在客户端发起模式(Client-Initiated)中，直接由支持L2TP协议的远程用户发起L2TP隧道连接，如图4-32所示。

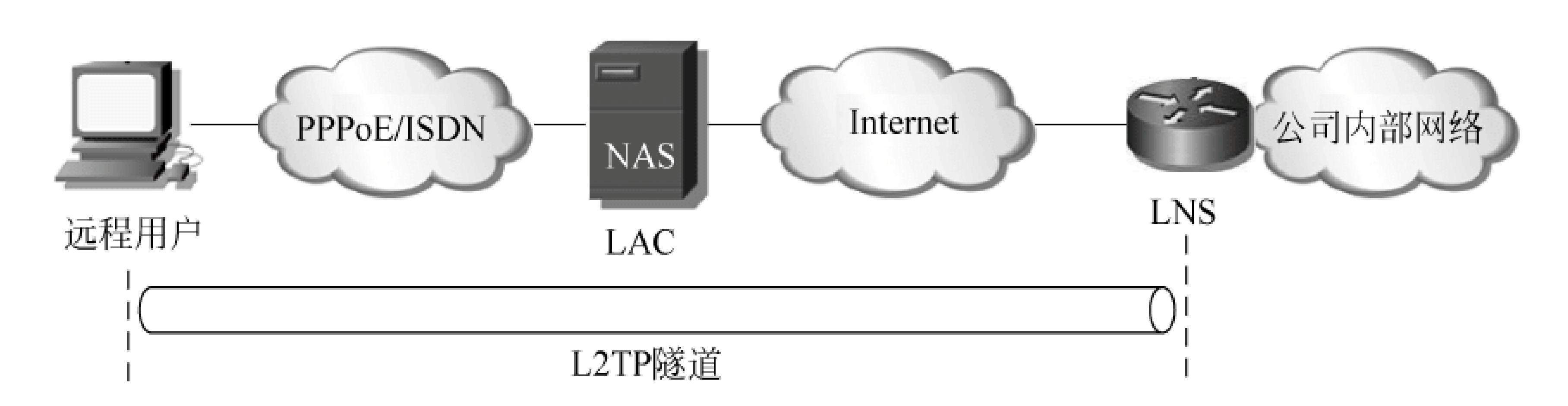


图4-32 Client-Initiated模式

远程用户在获得了访问Internet的权限后，直接向LNS发起隧道连接请求，并最终在远程用户和LNS之间建立L2TP隧道，无须经过一个单独的LAC设备来建立隧道。Client-Initiated模式要求远程用户系统支持L2TP协议，并且远程用户需要具有公网IP地址，能够直接通过Internet与LNS通信。

4. L2TP 的配置

在此依然以 H3C MSR 20-40 路由器为例介绍 L2TP VPN 的配置。路由器在 L2TP 中扮演着 LNS 的角色。在路由器的管理平台界面左侧的导航栏中选择“VPN>L2TP>L2TP 配置”，进入 L2TP 配置界面，如图 4-33 所示。

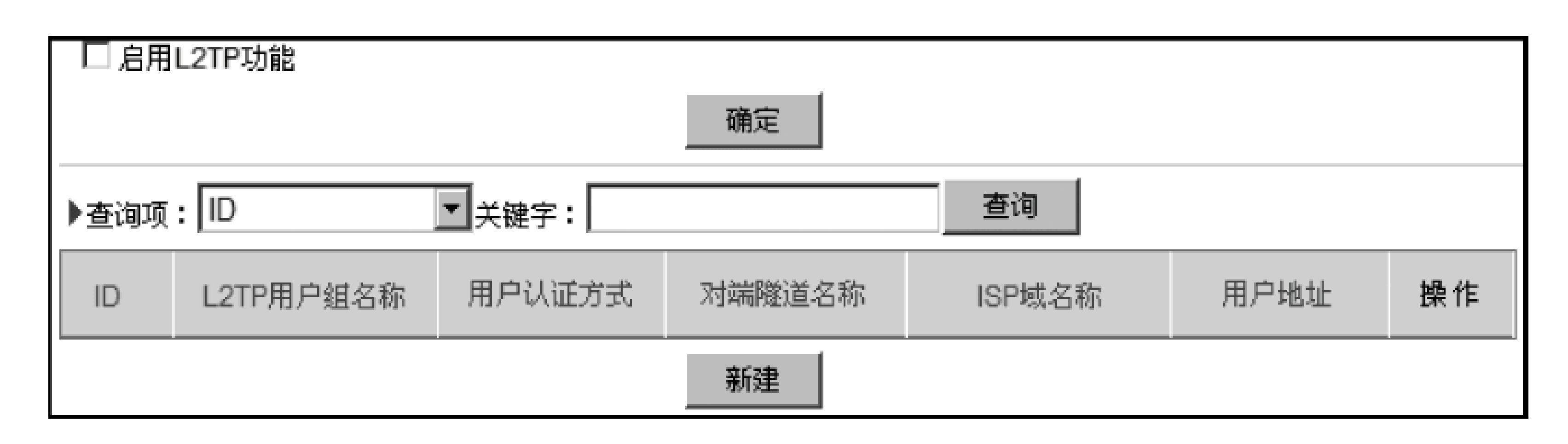


图 4-33　L2TP 配置界面

在“L2TP 配置”界面下选中“启用 L2TP 功能”复选框，并单击“确定”按钮，在路由器上启用 L2TP 的功能。单击“新建”按钮进入“新建 L2TP 用户组”界面，如图 4-34 所示。

新建L2TP用户组
L2TP配置
L2TP用户组名称：　*字符（1－15）
对端隧道名称：　字符（1－30）
本端隧道名称：　字符（1－30）
隧道验证：　启用
隧道验证密码：　字符（1－16）
PPP认证配置
PPP认证方式：　None
ISP域名：　新建　修改　删除
PPP地址配置
PPP Server 地址/掩码：　/　*
用户地址：　新建　修改　删除　强制分配地址：禁用
高级
Hello报文间隔：　60　秒（60－3600，缺省值＝60）
AVP数据隐藏：　禁用
流量控制：　禁用
强制本端CHAP认证：　禁用
强制LCP重协商：　禁用
星号（*）为必须填写项
确定　取消

图 4-34　新建 L2TP 用户组界面

L2TP 配置的参数项和具体的解释如下。

(1) L2TP 用户组名称：设置 L2TP 用户组的名称，该名称只有本地意义，定义一个容易区分和记忆的名字即可。

(2) 对端隧道名称：配置对端隧道的名称，在远程用户使用 Windows XP 自带的 VPN

客户端进行 L2TP 连接时,LNS 端不能配置该参数,否则会导致 L2TP 隧道无法建立。

(3) 本端隧道名称:配置本端隧道名称,本项可以不进行配置。

(4) 隧道验证:设置是否在该 L2TP 用户组中启用 L2TP 隧道验证功能。如果选择启用隧道验证,则应在 L2TP 隧道的两侧均启用该功能,并且要求两端的隧道验证密码必须一致,否则隧道将无法建立。为保证 L2TP 隧道的安全,建议最好启用隧道验证的功能。由于 Windows XP 不提供此项配置,因此在远程用户使用 Windows XP 自带的 VPN 客户端进行 L2TP 连接时,LNS 端必须选择禁用隧道验证功能。

(5) PPP 认证方式:L2TP 依赖于 PPP 协议提供的认证功能来确保连接的安全性。PPP 认证方式可以选择 None、PAP 和 CHAP,分别表示不进行认证、使用密码验证协议(Password Authentication Protocol,PAP)进行认证和使用质询握手验证协议(Challenge Handshake Authentication Protocol,CHAP)进行认证。建议选择比较安全的 CHAP 认证方式。

(6) ISP 域名:设置用户进行 PPP 认证所采用的 ISP 域的名称。默认域为 system,可以单击"新建"按钮进入"新建 ISP 域"界面,新建一个 ISP 域,也可以使用系统默认的 system 域并单击"修改"按钮进入"修改 ISP 域"界面对其进行修改。新建 ISP 域界面和修改 ISP 域界面基本相同,新建 ISP 域界面如图 4-35 所示。

新建ISP域
ISP域名称: *字符(1-24)
PPP认证方案:
主用方案 服务器类型 Local 方案名称
备选方案 禁用
PPP授权方案:
主用方案 服务器类型 Local 方案名称
备选方案 禁用
PPP计费方案: 计费开关 禁用
主用方案 服务器类型 Local 方案名称
备选方案 禁用
最大用户数: (1-2147483646)
星号(*)为必须填写项
确定 取消

图 4-35 新建 ISP 域界面

在"新建 ISP 域"或"修改 ISP 域"界面下主要进行 PPP 认证、授权和计费方案的配置。PPP 认证方案、授权方案和计费方案中的服务器类型可以选择 None、Local 和 Radius。其中,None 表示不认证/直接授权/不计费,Local 表示采用本地认证/授权/计费,Radius 表示采用 Radius 进行认证/授权/计费。关于认证、授权和计费以及 Radius 部分会在第 6 章局域网安全的 AAA 技术部分进行详细讲解。在此只要 PPP 认证方案使用系统默认的服务器类型 Local 即可,即在本地进行 PPP 认证。

(7) PPP Server 地址/掩码:设置本端的 IP 地址和子网掩码。LNS 端一般会从企业内部网段中专门划分出一个 IP 地址段来为远程用户分配企业内部 IP 地址,此处配置的 PPP Server 地址即为该网段中的一个 IP 地址,该地址会分配到路由器的虚拟模板接口

(Virtual-Template)上,并通过该虚拟模板接口为远程用户分配本网段的 IP 地址。需要注意的是,为远程用户分配的是一个独立的 IP 网段,因此 PPP Server 地址不能与路由器的物理接口地址所在网段冲突;另外,企业内部网络中的其他路由器或三层交换机的路由表中必须存在去往 PPP Server 地址所在网段的路由,否则会导致远程用户无法访问企业内部网络中的某些部分。

(8) 用户地址:设置给远程用户分配企业内部 IP 地址所用的地址池或直接给远程用户分配指定的 IP 地址。下拉框中显示第(6)项配置的 ISP 域下的地址池,可以单击“修改”按钮进入“修改地址池”界面对已有的地址池进行修改,也可以单击“新建”按钮进入“新建地址池”界面,新建一个地址池。新建地址池界面和修改地址池界面基本相同,新建地址池界面如图 4-36 所示。

新建地址池
域名:
地址池编号: *(0-99)
开始地址: *
结束地址:
星号(*)为必须填写项
确定　取消

图 4-36　新建地址池界面

其中,域名用来设置地址池所在的 ISP 域,此处设置的域名要与第(6)项设置的 ISP 域名相同。地址池编号给出一个 0～99 的编号即可。开始地址和结束地址用来设置地址池的地址范围,开始地址和结束地址之间的地址数不能超过 1024 个,如果只设置了开始地址,则表示地址池中只有开始地址这一个地址。

(9) 强制分配地址:设置是否强制对端使用本端为其分配的 IP 地址,即不允许对端使用自行配置的 IP 地址。

(10) Hello 报文间隔:设置发送 Hello 报文的时间间隔。LAC 和 LNS 之间会定期向对端发送 Hello 报文,接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定的时间间隔内未收到对端的 Hello 响应报文,则将重复发送 Hello 报文,如果重复发送 3 次仍未收到对端的响应报文,则断开隧道连接。

(11) AVP 数据隐藏:设置是否采用隐藏方式传输属性值对(Attribute Value Pair,AVP)数据。L2TP 协议的一些参数通过 AVP 数据来进行传输,如果用户对这些数据的安全性要求比较高,可以将 AVP 数据的传输方式设置为隐藏传输,即对 AVP 数据进行加密,该配置项仅在 LAC 端配置有效。

(12) 流量控制:设置是否启用 L2TP 隧道流量控制功能,该功能应用在数据报文的发送和接收过程中。启用流量控制功能后,会对接收到的乱序报文进行缓存和调整。

(13) 强制本端 CHAP 认证和强制 LCP 重协商:设置 LNS 侧的用户认证方式。在 L2TP 组网中 LNS 侧的用户认证方式有 3 种:强制本端 CHAP 认证、强制 LCP 重协商和代理认证。

强制本端 CHAP 认证:启用此功能后,对于由 NAS 发起隧道连接的 VPN 用户端会

经过两次认证。一次是用户端在NAS端的认证,另一次是用户端在LNS端的CHAP认证。

强制LCP重协商:对由NAS发起隧道连接的PPP用户端,在PPP会话开始时,用户先和NAS进行PPP协商。若协商通过,则由NAS初始化L2TP隧道连接,并将用户信息传递给LNS,由LNS根据收到的代理验证信息,判断用户是否合法。但在某些特定情况下(如在LNS侧也要进行认证与计费),则需要强制LNS与用户间重新进行LCP协商,此时将忽略NAS侧的代理认证信息。

代理认证:如果强制本端CHAP认证和强制LCP重协商功能都不启用,则LNS对用户进行的是代理认证。在这种情况下,LAC将它从用户得到的所有认证信息及LAC端本身配置的认证方式发送给LNS。

三种认证方式中,优先级顺序依次是"强制LCP重协商>强制本端CHAP认证>代理认证",默认采用代理认证方式。

在L2TP配置完成后,还有一项需要进行配置,那就是需要新建一个用户。这是因为L2TP依赖于PPP协议提供的认证功能来确保连接的安全性,而ISP域中配置的PPP认证方案中服务器类型为Local,即在路由器本地进行远程用户的认证,因此需要在路由器上新建一个用户,使用该用户的用户名和密码对远程用户进行认证。

在路由器的管理平台界面左侧的导航栏中选择"系统管理>用户管理",进入用户管理界面,在用户管理界面下单击创建用户,进入创建用户界面,如图4-37所示。

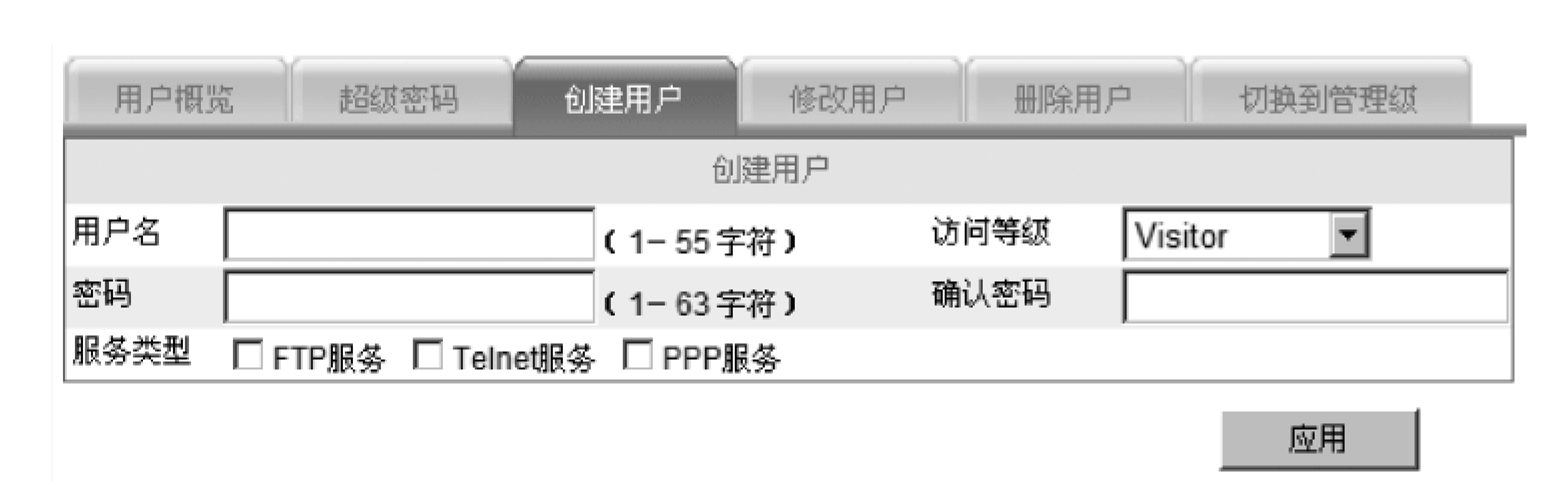


图4-37 创建用户界面

创建一个用户,其访问等级设置为Configure,服务类型选中"PPP服务"复选框,然后单击应用按钮即可。

(1) 仅L2TP隧道配置。

假设存在如图4-38所示的网络,网络联通性已经配置完成。要求配置L2TP协议,使PC_1可以通过L2TP隧道访问企业内部网络。其中PPP认证方式采用CHAP,用户名和密码分别是abc和123456;为远程用户分配的IP地址段为10.1.2.0/24。



图4-38 L2TP配置网络拓扑结构

从图 4-38 中可以看出，这是一个典型的客户端发起模式的 L2TP 网络。为简单起见，将远程主机直接连接到 LNS 上，省略掉 LAC 设备和中间的网络。

在配置之前，首先需要保证路由器 RTB 上存在去往网络 10.1.2.0/24 的路由。路由器 RTA（即 LNS）上 L2TP 协议的具体配置如图 4-39～图 4-42 所示。

新建L2TP用户组

L2TP配置

L2TP用户组名称：	111	*字符（1－15）
对端隧道名称：		字符（1－30）
本端隧道名称：		字符（1－30）
隧道验证：	禁用	
隧道验证密码：		字符（1－16）

PPP认证配置

PPP认证方式：	CHAP	
ISP域名：	system	新建 修改 删除

PPP地址配置

PPP Server 地址/掩码：	10.1.2.1 / 255.255.255.0	*
用户地址：	pool1	新建 修改 删除 强制分配地址：禁用

□ 高级

星号（*）为必须填写项

图 4-39 L2TP 配置

用户概览 超级密码 创建用户 修改用户 删除用户 切换到管理级

创建用户

用户名	abc	（1－55字符）	访问等级	Configure
密码	••••••	（1－63字符）	确认密码	••••••
服务类型	□ FTP服务 □ Telnet服务 ☑ PPP服务			

应用

图 4-40 创建用户

在远程主机 PC_1 上需要新建一个 VPN 连接。在“网上邻居—属性”界面下的左上角“网络任务”中单击“创建一个新的连接”按钮，使用新建连接向导创建连接。其中“网络连接类型”选择“连接到我的工作场所的网络（O）”单选按钮，如图 4-43 所示。

在“网络连接”对话框中选择“虚拟专用网络连接（V）”单选按钮，如图 4-44 所示。

在“连接名”对话框中为本连接定义一个名字，如图 4-45 所示。

注意：*该名字只有本地意义，与隧道名称无关。*

“公用网络”对话框中选择“不拨初始连接（D）”，如图 4-46 所示。

“VPN 服务器选择”对话框中输入 LNS 的 IP 地址，在此输入 LNS 中配置的 PPP Server 地址 10.1.2.1 或者 LNS 路由器 E0/0 接口的地址 202.207.120.1 均可，如图 4-47 所示。

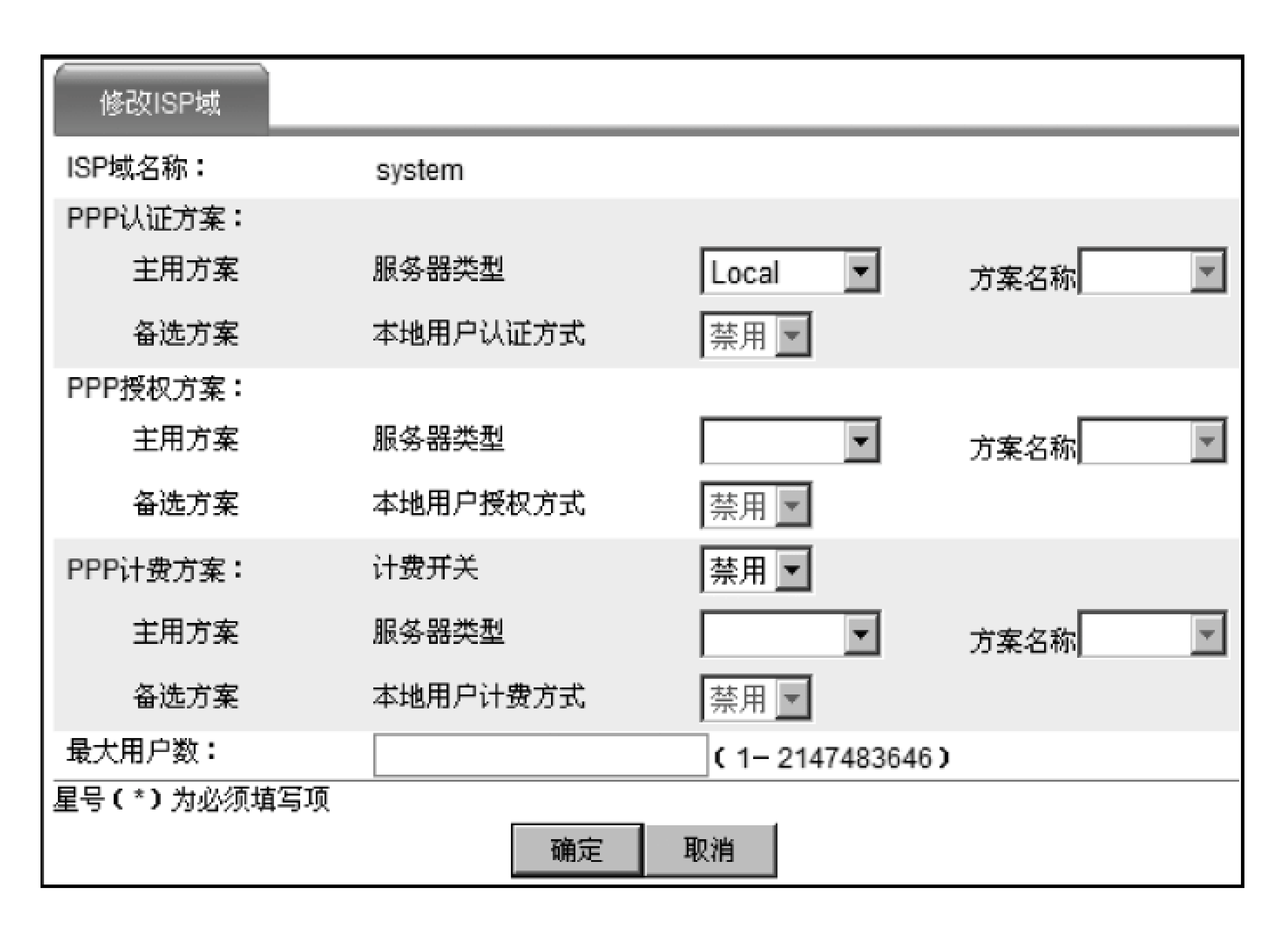


图 4-41 修改默认 system 域配置

新建地址池

域名： system

地址池编号： 1 *(0-99)

开始地址： 10.1.2.2 *

结束地址： 10.1.2.254

星号(*)为必须填写项

确定 取消

图 4-42 新建为远程用户分配地址的地址池

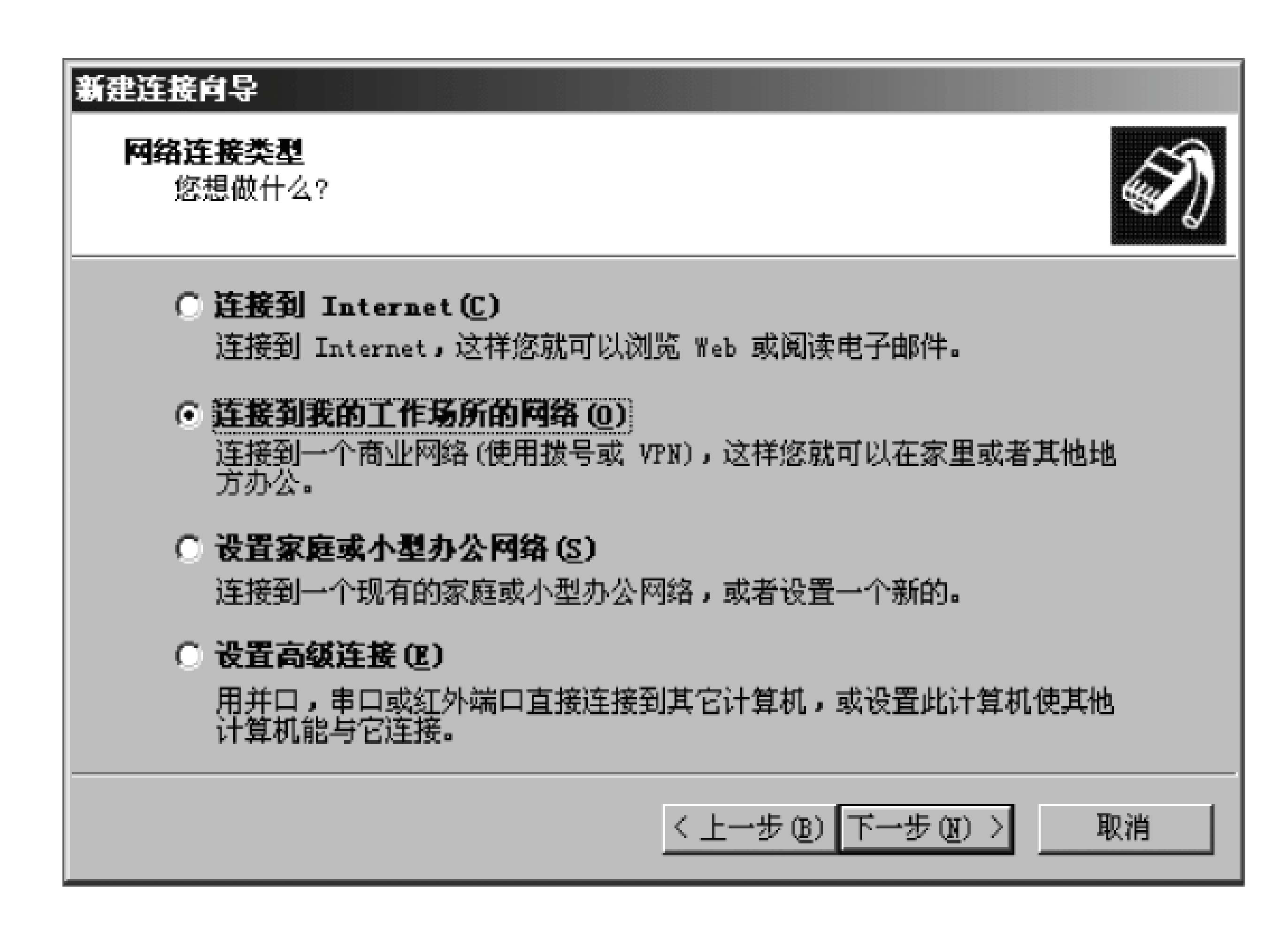


图 4-43 选择网络连接类型

完成连接的创建后，在该连接属性中的“网络”选项卡中选择“VPN 类型”为“L2TP IPSec VPN”，如图 4-48 所示。如果 VPN 类型选择为“自动”，则同样会与 LNS 端通过协

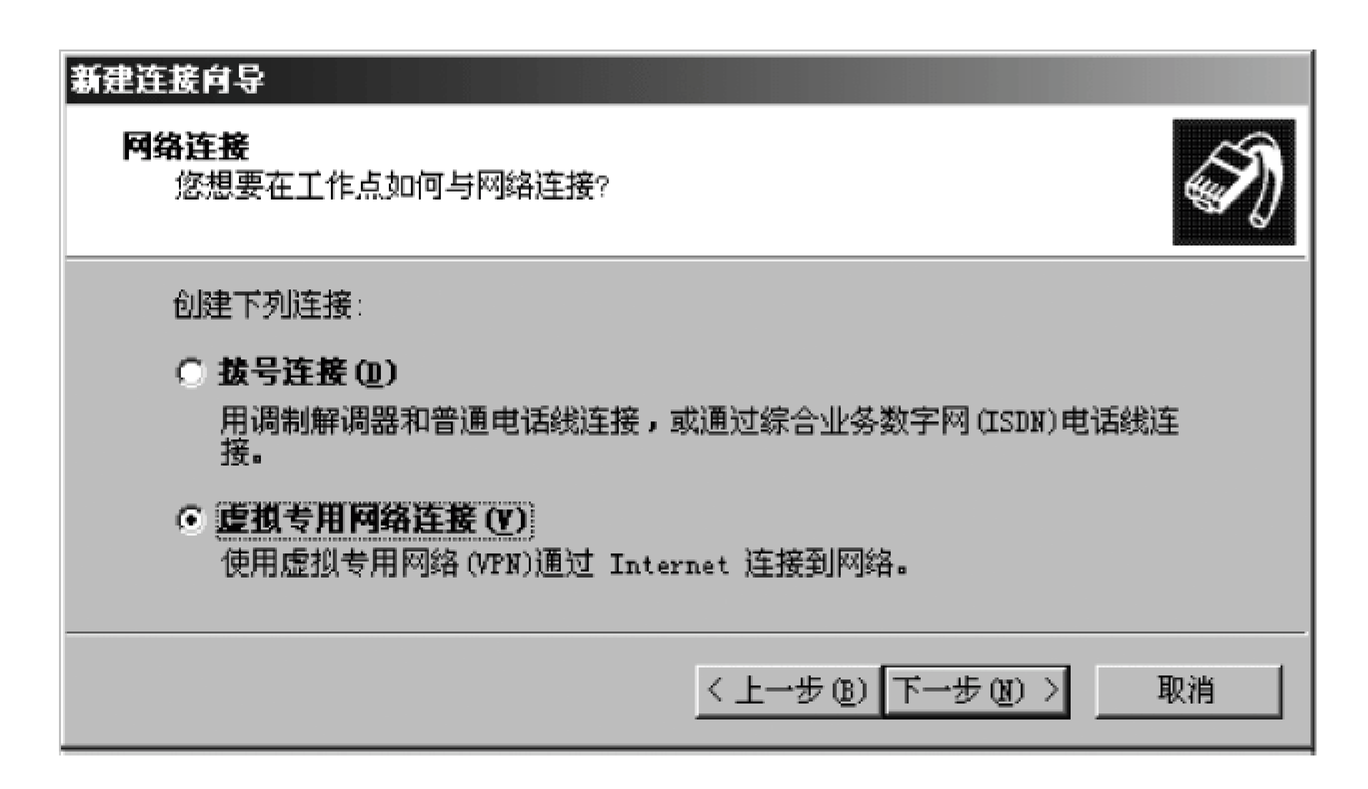


图 4-44　选择网络连接方式

图 4-45　指定连接名称

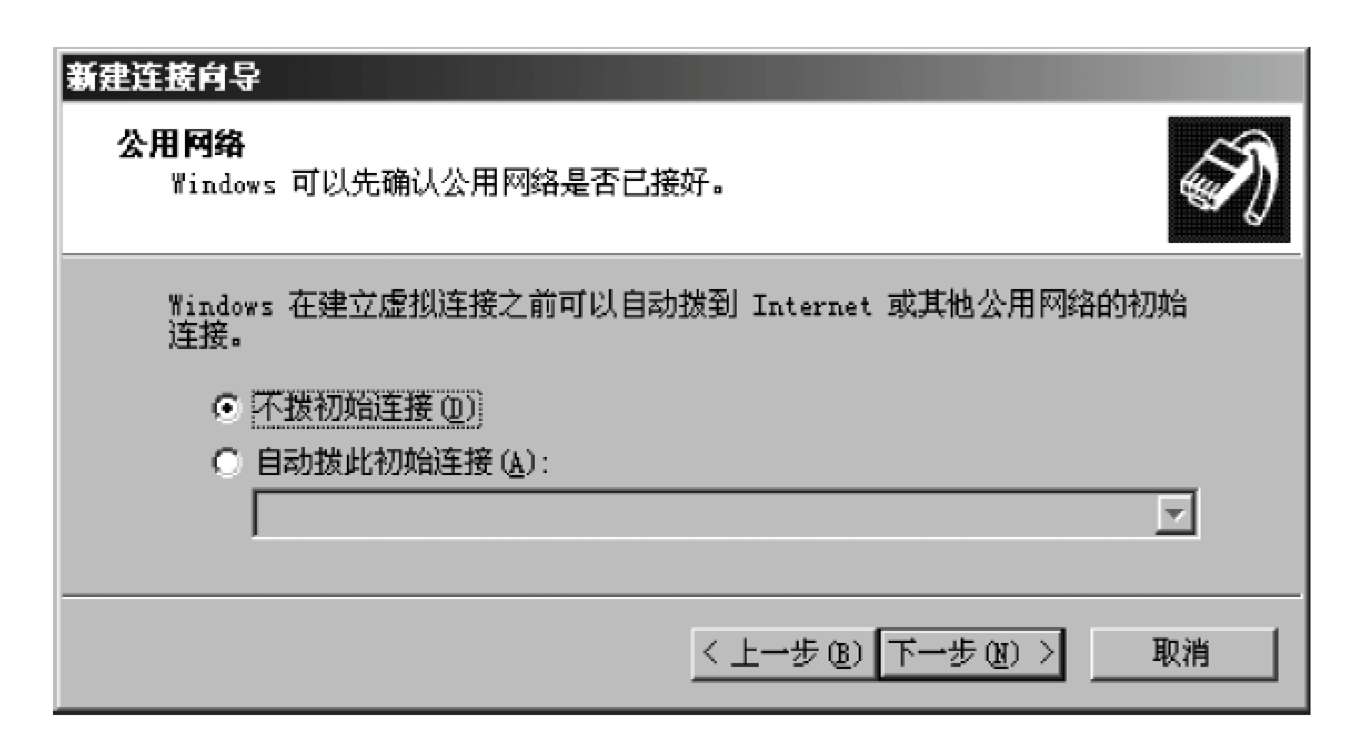


图 4-46　公用网络选择

商使用 L2TP IPSec VPN。其他配置均使用默认配置即可。

由于 VPN 类型使用的是“L2TP IPSec VPN”，因此 PC_1 上会要求对数据进行 IPSec 封装，而在 LNS 端只配置了 L2TP，所以需要在 PC_1 上修改注册表的配置，使 PC_1 忽略 IPSec 功能。具体如下：在命令行模式下执行 regedit 命令，弹出“注册表编辑器”对话框。在左侧注册表项目中逐级找到“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters”，单击 Parameters 参数，接着在右边

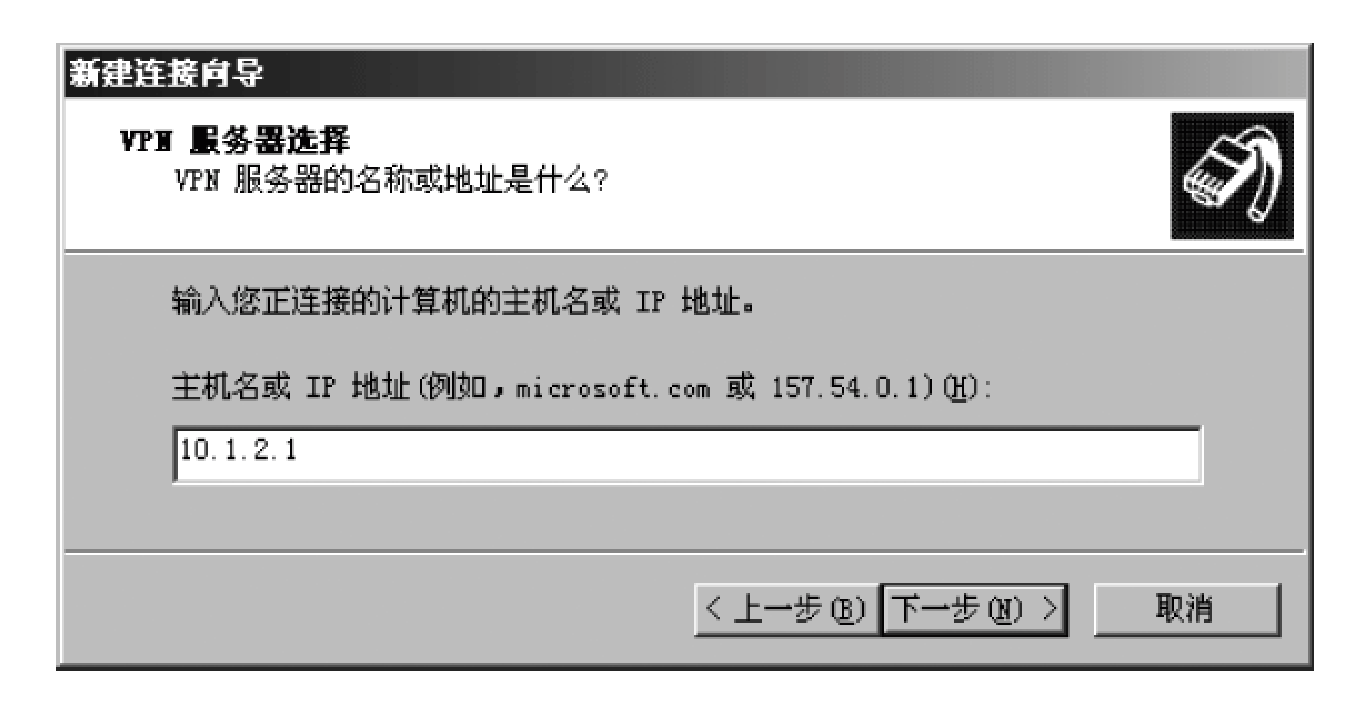


图 4-47 VPN 服务器地址配置

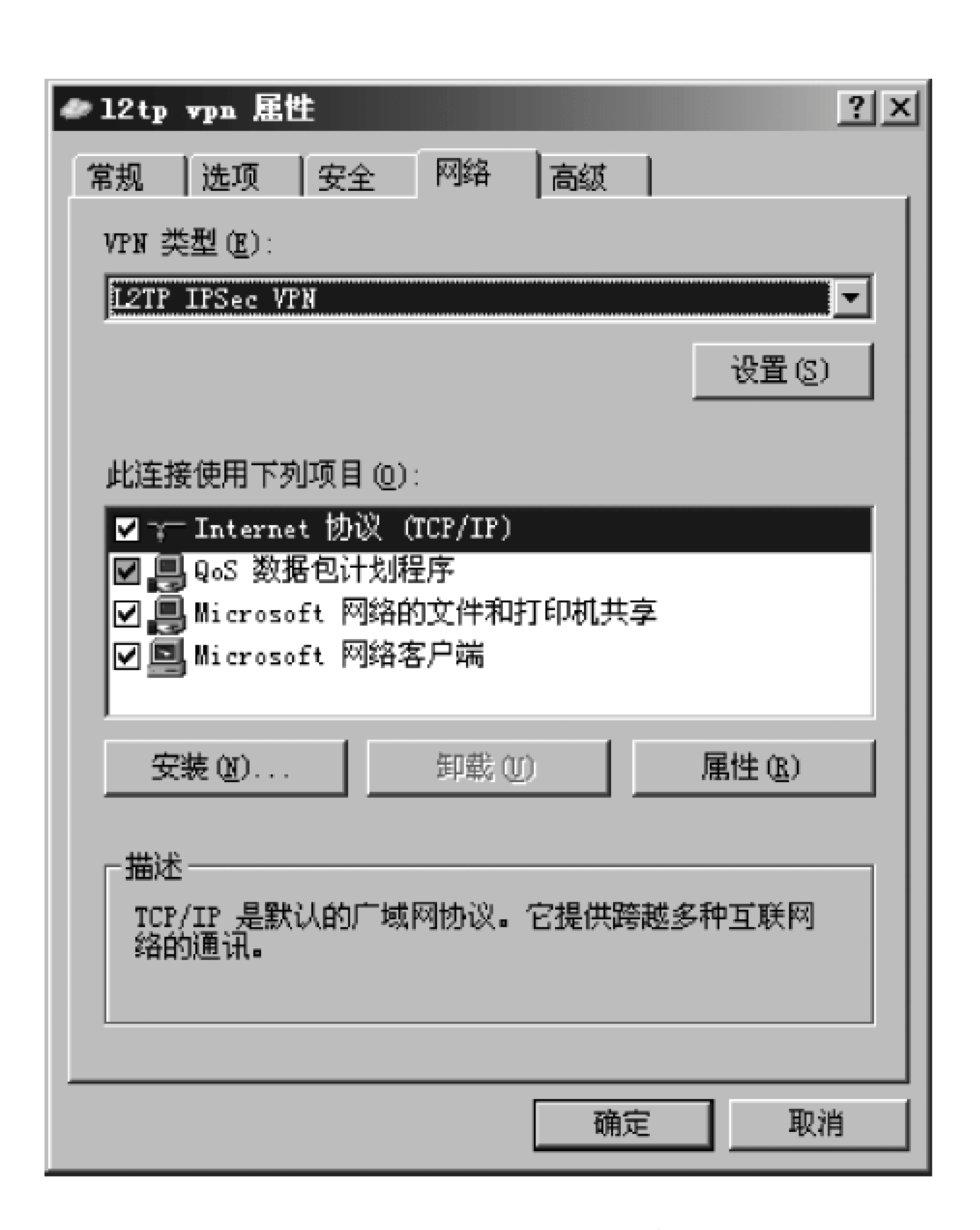


图 4-48 选择 VPN 类型

窗口空白处右击，在弹出窗口中逐级选择“新建/DWORD值”新建一个注册表值，将其命名为ProhibitIPSec，值设置为1，如图4-49和图4-50所示。重新启动Windows。

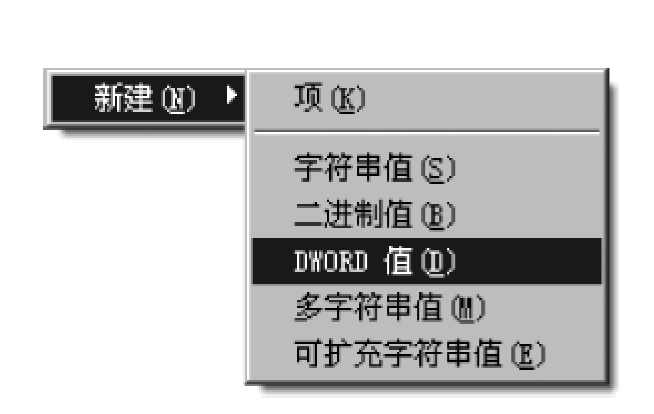


图 4-49 新建注册表值



图 4-50 设置注册表值名称和数据

PC_1 重新启动后，在新建的连接上右击，在弹出的快捷菜单中选择“连接”，出现 VPN 连接对话框，在对话框中输入用户名 abc 和密码 123456，单击“连接”按钮，即可与 LNS 之间建立 L2TP 隧道连接，如图 4-51 所示。



图 4-51　PC_1 发起 L2TP 连接

L2TP 连接建立后，在路由器 RTA 上的 L2TP 隧道信息界面中可以看到已建立的 L2TP 隧道的信息，如图 4-52 所示。

本端隧道编号	对端隧道编号	对端隧道端口	对端隧道IP地址	会话数目	对端隧道名称	操作
1	10	1701	202.207.120.2	1	teacher049	

刷新

图 4-52　L2TP 隧道信息

此时，在 PC_1 上使用 ipconfig 命令查看 IP 地址如下：

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 202.207.120.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 202.207.120.1
PPP adapter l2tp vpn:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.2.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 10.1.2.2
```

从显示的结果可以看出，PC_1 获得了企业内部网络地址 10.1.2.2，需要注意的是对

于 L2TP VPN 连接,默认网关给出的地址与 PC_1 获得的 IP 地址相同,同样是 10.1.2.2。

从 PC_1 上使用 ping 命令可以联通企业内部主机 PC_2,在使用 ping 命令测试的同时,在 PC1 上使用 Wireshark 软件捕获数据报文,如图 4-53 所示。

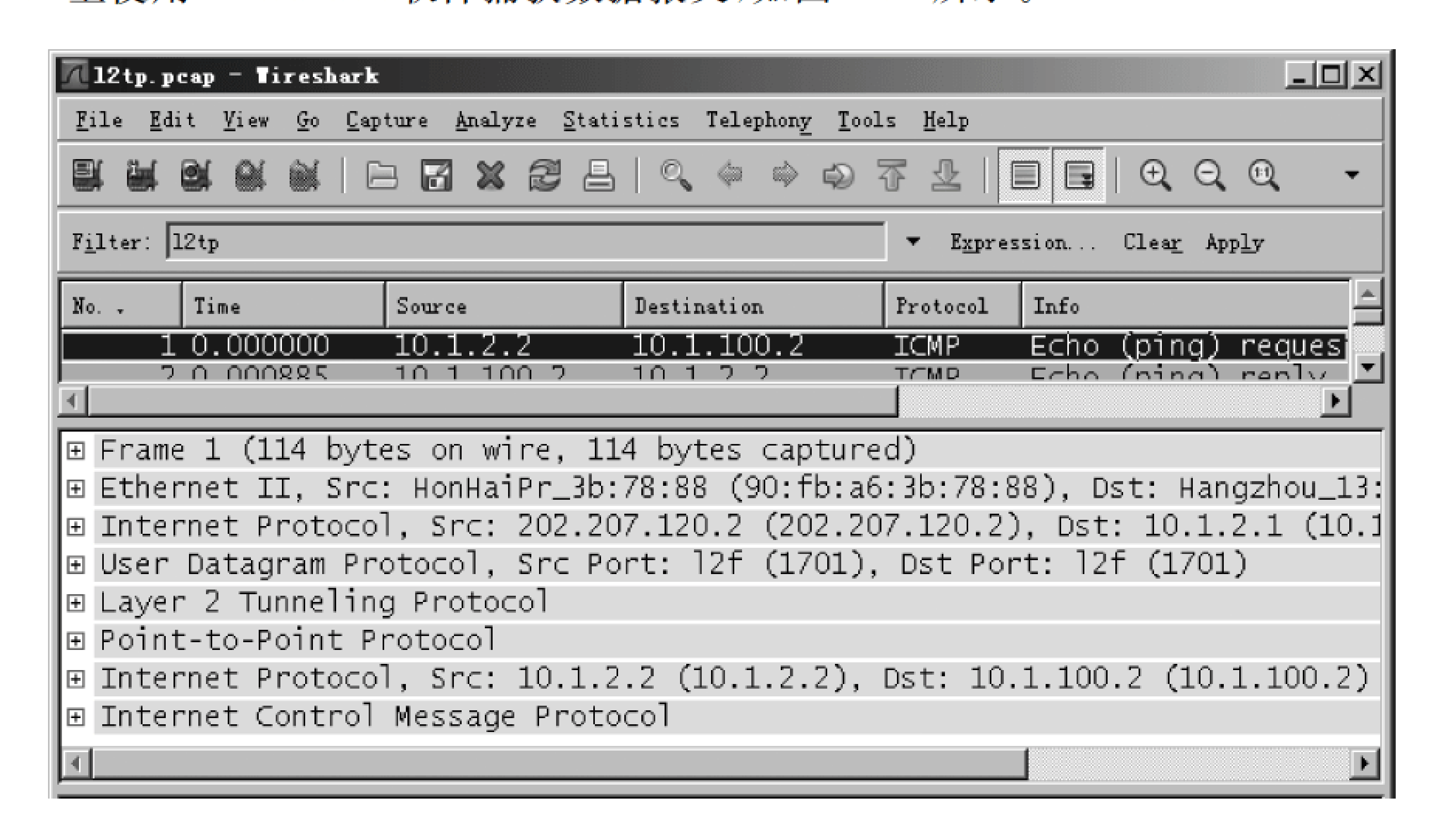


图 4-53 PC_1 上 L2TP 数据报文

从图 4-53 中可以看到 PC_1 上的 L2TP 数据报文,其中内部 IP 报头中的源 IP 地址和目的 IP 地址分别为 PC_1 和 PC_2 的企业内部地址 10.1.2.2 和 10.1.100.2;外部 IP 报头中的源 IP 地址为 PC_1 的公网地址 202.207.120.2,目的地址为 LNS 的 PPP Server 地址 10.1.2.1,如果在图 4-46 中给出的 LNS 地址为路由器 RTA 的 E0/0 接口的 IP 地址 202.207.120.1,则外部 IP 报头中的目的地址将变成 202.207.120.1。

(2) L2TP+IPSec 隧道配置。

L2TP 协议通过对远程用户进行身份认证为其与 LNS 之间建立一条隧道进行数据的传输,但 L2TP 协议并不提供数据的加密和认证功能。因此在实际应用中往往将 L2TP 与 IPSec 结合起来使用,用以为远程用户与企业内部网络之间的流量进行加密。

在此依然使用图 4-38 所示的网络,在已经配置了 L2TP 的基础上,要求增加 IPSec 配置,以实现数据的加密和认证,预共享密钥为 123。

在配置之前,首先将 PC_1 的公网 IP 地址修改为 202.207.120.0/24 网段的另外一个地址,然后登录路由器 RTA 进行 IPSec 配置,以避免配置 IPSec 后无法登录路由器 RTA。IPSec 的具体配置如图 4-54 所示。

部分配置项的具体解释如下。

① 对端网关地址/主机名:IPSec 配置中必须要给出对端网关地址,在此配置的是远程用户的公网 IP 地址范围。在本例中,远程用户只有 202.207.120.2,因此对端网关地址直接指定 202.207.120.2 即可。但是在实际网络中,远程用户 IP 地址并不固定,因此需要指定一个 IP 地址的范围,而在 Web 配置界面下只能指定单个 IP 地址,此时就需要在命令行模式下对对端网关地址范围进行修改。

假设需要指定对端网关地址范围为 202.207.120.2～202.207.120.254,则可首先在

新建IPSec连接

IPSec连接名称 123

网关信息

接口 Ethernet0/0

组网模式 ⊙站点到站点 ○PC到站点

网关地址

对端网关地址/主机名 202.207.120.2 字符（1-255）

本端网关地址

认证

认证方式

⊙预共享密钥 ●●● *字符（1-128）

○证书

网关ID

对端ID类型 ⊙IP地址 ○网关名称

本端ID类型 ⊙IP地址 ○网关名称

筛选器

筛选方式 流量特征

源地址/通配符 0.0.0.0 / 255.255.255.255 *

目的地址/通配符 202.207.120.2 / 0.0.0.0 *

▼高级

第一阶段

交换模式 ⊙主模式 ○野蛮模式

认证算法 SHA1

加密算法 DES

DH Diffie-Hellman Group1

SA的生存周期 86400 秒（60-604800，缺省值=86400）

第二阶段

协议 ESP

ESP认证算法 MD5

ESP加密算法 3DES

封装模式 ○隧道模式 ⊙传输模式

PFS None

SA的生存周期

基于时间的生存周期 3600 秒（180-604800，缺省值=3600）

基于流量的生存周期 250000 千字节（2560-4294967295，缺省值=1843200）1843200）

DPD ○开启 ⊙关闭

选择加密卡 << >>

星号（*）为必须填写项

确定 取消

图 4-54 与 L2TP 结合的 IPSec 配置

Web 界面下配置对端网关地址为任意一个地址或不配置对端网关地址。在 Web 界面下对 IPSec 配置完成后，使用超级终端登录路由器，执行 display current-configuration 命令，显示结果如下：

```
[RTA]display current-configuration
----------output omitted----------
#
ike peer 123
proposal 1
pre-shared-key cipher TEzJOUGCmuE=
remote-address 202.207.120.2
nat traversal
#
----------output omitted----------
```

从上面的显示结果可以看出,在 Web 界面下配置了对端网关地址为 202.207.120.2,修改其地址范围为 202.207.120.2~202.207.120.254 的命令如下:

```
[RTA]ike peer 123
[RTA-ike-peer-123]remote-address 202.207.120.2 202.207.120.254
```

② 源地址/通配符:由于远程用户需要访问企业内部网络,因此源地址/通配符配置的是允许远程用户访问的企业内部网络的地址范围。如果允许远程用户访问企业内部网络的任何部分,可以简单地将其设置为 0.0.0.0/255.255.255.255。

③ 目的地址/通配符:设置远程用户的公网 IP 地址范围,即哪些 IP 地址的公网用户可以匹配 IPSec 策略。此项配置与对端网关地址的配置类似,一般也是一个地址范围,而且地址范围应与对端网关地址范围完全相同。但为了简单起见,在本例中将其设置为一个 IP 地址 202.207.120.2,这是因为如果设置为 202.207.120.0/0.0.0.255,则 PC_1 配置为 202.207.120.0/24 网段的任何一个地址其流量均会触发该筛选器,使路由器要求建立 IPSec 隧道,而 PC_1 此时只有本地连接,从而导致 PC_1 无法连接到路由器。这也是在进行 IPSec 配置之前修改 PC_1 的 IP 地址的原因。

④ 第一阶段的加密算法和 DH:由于 Windows XP 系统只支持 DES 和 3DES 两种加密算法以及 Diffie-Hellman Group1 和 Diffie-Hellman Group2 两种 DH 算法,因此第一阶段的加密算法和 DH 算法必须要选择 PC_1 上的 Windows XP 系统支持的算法。

⑤ 第二阶段的加密算法:同样只能选择 DES 和 3DES 两种加密算法。

⑥ 封装模式:必须选择 IPSec 的封装模式为传输模式。

⑦ 基于流量的生存周期:为与 PC_1 上的 Windows XP 系统相匹配,第二阶段 SA 的基于流量的生存周期必须设置为 250000。

路由器上配置完成后,先将 PC_1 的公网 IP 地址修改回 202.207.120.2,然后进行一些配置上的修改。

① 将上一节中增加的注册表参数 ProhibitIPSec 删除或将其值修改为 0,并重新启动计算机,使 PC_1 具备 IPSec 的功能。

② 在 PC_1 上启动 IPSec Services 服务,如图 4-55 所示。

(3) 在上一节创建的 VPN 连接属性中的“安全”选项卡中单击“IPSec 设置”按钮,在弹出的对话框中选中“使用预共享的密钥做身份验证”复选框,并输入预共享密钥 123,如图 4-56 所示。



图 4-55　启动 IPSec Services 服务



图 4-56　输入预共享密钥

配置完成后，在 VPN 连接上右击，在弹出的快捷菜单中选择“连接”，出现 VPN 连接对话框，在对话框中输入用户名 abc 和密码 123456，单击“连接”按钮，即可与 LNS 之间建立 L2TP+IPSec 的隧道连接。

连接建立后，从 PC_1 上使用 ping 命令可以联通企业内部主机 PC_2，在使用 ping 命令测试的同时，在 PC_1 上使用 Wireshark 软件捕获数据报文，如图 4-57 所示。

从图 4-57 中可以看出，L2TP 报文被 ESP 协议加密封装，外部 IP 报头没有改变。

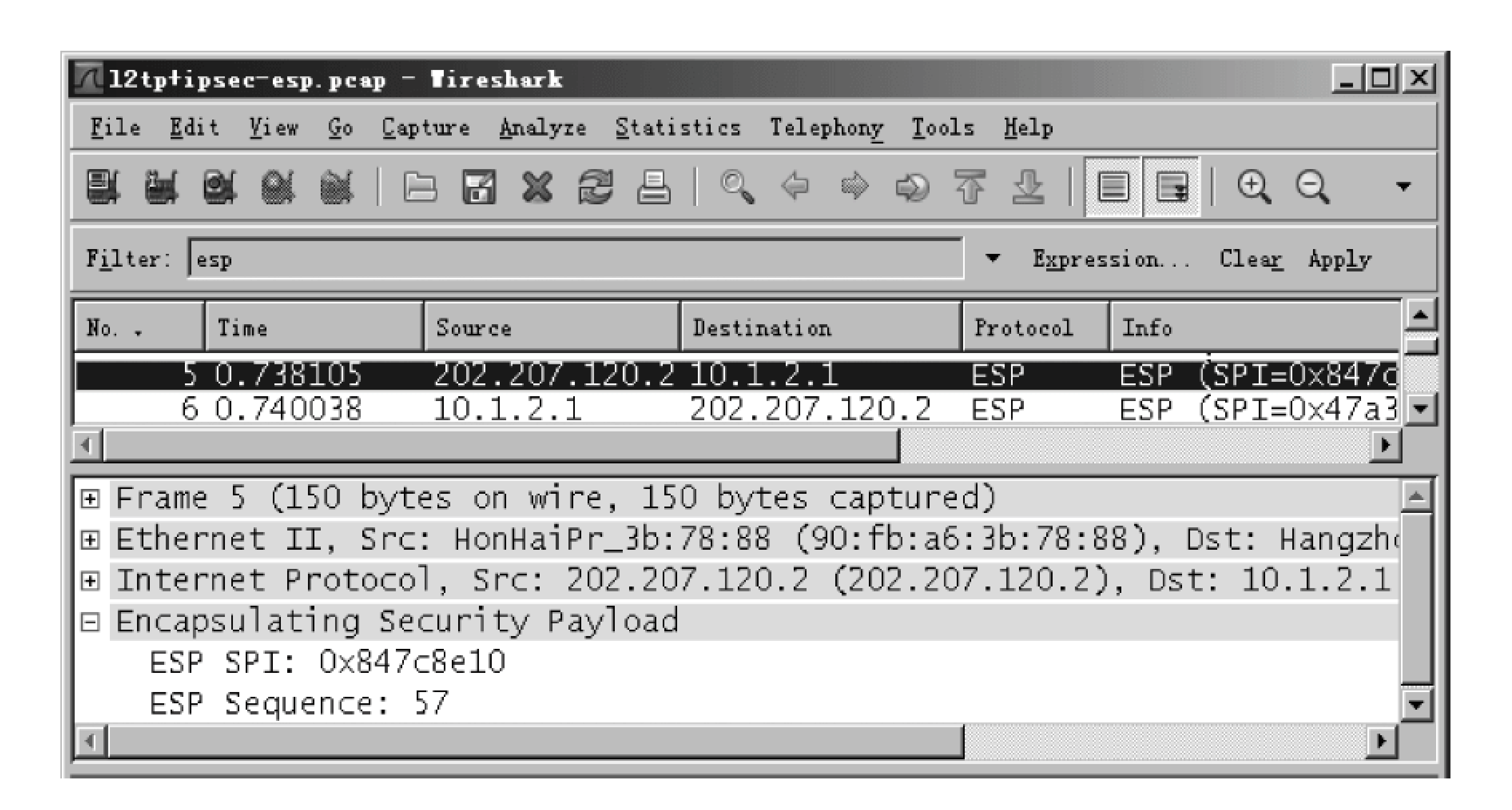


图 4-57 PC$_1$ 上 L2TP＋IPSec 数据报文

L2TP＋IPSec 封装的报文结构如图 4-58 所示。

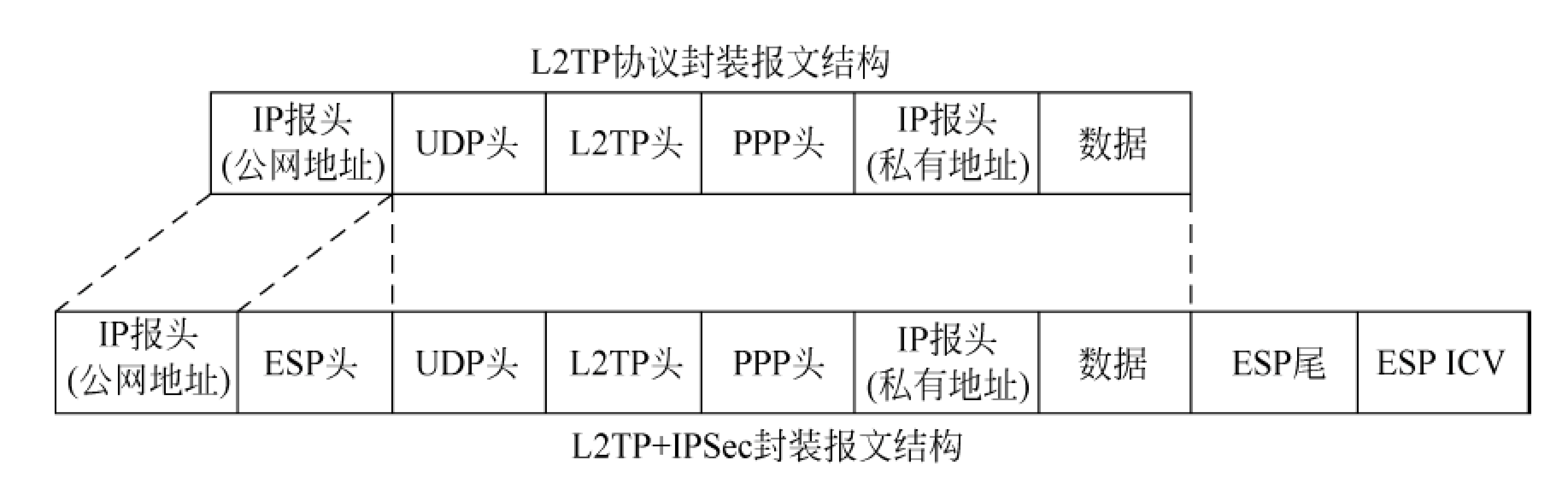


图 4-58 L2TP＋IPSec 封装报文结构

图 4-58 与图 4-13 相对应，ESP 协议将 L2TP 的封装作为传输层报文进行了加密和认证，保持原始的外部 IP 报头不变。这也解释了在图 4-54 中进行 IPSec 配置时“对端网关地址/主机名”和“目的地址/通配符”中为什么配置的均为远程用户的公网 IP 地址范围，而不是为远程用户分配的企业内部 IP 地址范围。

注意：在建立了 L2TP＋IPSec 隧道连接后，PC$_1$ 将无法 ping 通路由器 RTA 的 E0/0 接口的 IP 地址 202.207.120.1，但可以 ping 通路由器 RTA 的 E0/1 接口的 IP 地址 10.1.1.1以及企业内部网络中的所有 IP 地址。

4.4.2 Easy VPN

在 Cisco 设备上，远程访问 VPN 一般采用 Easy VPN 的方式实现。Easy VPN 的架构包括如下两部分。

(1) 在网络设备上的远程访问 VPN 服务器。

(2) Cisco Easy VPN Remote，如在远程用户计算机上的 Cisco VPN 客户端软件、Easy VPN 硬件客户端或在网络设备上配置的 Easy VPN 客户端。

Easy VPN 将大量 VPN 通信的管理工作，如定义大量 VPN 通信参数、对远端 VPN

对等体进行失效检查等，集中在 VPN 服务器一端进行。因此与站到站 VPN 不同，实施 Easy VPN 时，VPN 服务器和 VPN 客户端的配置操作有很大区别。

1. Easy VPN 服务器配置

与站到站 VPN 相比，Easy VPN 为简化在客户端的配置，除提供建立 VPN 安全隧道的基本功能外，还提供以下功能：

(1) 一旦 VPN 安全通道建立成功，Easy VPN 服务器可以为远程访问用户分配访问公司内部网络的 IP 地址，使其可以像使用专用线路一样访问公司网络，并自动建立 NAT 或 PAT，关联必要的 ACL。

(2) 对用户身份进行认证，以对其进行访问控制。

(3) 由 Easy VPN 服务器端将 VPN 安全通道的各项参数作为组策略推送到 VPN 客户端。

Easy VPN 服务器与 Easy VPN 客户端之间对等体的会话步骤如下：

(1) 使用 ISAKMP 在 Easy VPN 服务器与 Easy VPN 客户端间进行认证。

(2) 使用 IKE 扩展认证(IKE Extended Authentication，XAuth)对用户身份进行认证。

(3) 通过认证后，VPN 服务器向 VPN 客户端推送组策略。

(4) 创建 IPSec SA。

由于以上所述变换，在 Easy VPN 服务器一端，除需要进行 ISAKMP 策略、变换集和加密图的定义以及应用加密图等操作外，还需要以下配置操作：

(1) 增加 IP 地址池等有关配置。

(2) 增加用户身份认证、授权的配置。

(3) 增加推送组策略的定义。

(4) 将所定义的身份认证、授权等与加密图绑定在一起。

Easy VPN 服务器端配置涉及的命令如下。

(1) 创建为远程用户分配企业内部 IP 地址的地址池。

```
Router(config)#ip local pool {default|pool-name low-ip-address high-ip-address}
```

(2) 为远程用户配置 AAA 策略。

```
Router(config)#aaa new-model
Router(config)#aaa authentication login list-name local [method1[method2]]
Router(config)#aaa authorization network list-name local [method1[method2]]
```

关于 AAA 技术将在第 6 章进行详细介绍，在此认证和授权方案采用 Local 即可，即采用本地认证和授权。因此还需要在路由器上配置用户名和密码，以供远程用户登录认证使用。具体命令如下：

```
Router(config)#username username password password
```

(3) 为远程用户访问创建 IKE 策略。

```
Router(config)#crypto isakmp policy priority
```

```
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption {des|3des|aes}
Router(config-isakmp)#group 2
Router(config-isakmp)#hash {md5|sha}
Router(config-isakmp)#lifetime lifetime
```

在 Easy VPN 配置 IKE 策略时,group 只能配置为 2。

(4) 创建推送到客户端的组策略。

```
Router(config)#crypto isakmp client configuration group group-name
Router(config-isakmp-group)#key key-string
Router(config-isakmp-group)#pool pool-name
Router(config-isakmp-group)#dns dns-ip-address
Router(config-isakmp-group)#domain domain-name
Router(config-isakmp-group)#netmask netmask
```

其中,预共享密钥和地址池必须进行配置。

(5) 创建一个变换集。

```
Router(config)#crypto ipsec transform-set transform-set-name
{ah-md5-hmac|ah-sha-hmac|esp-des|esp-3des|esp-aes|esp-md5-hmac|esp-sha-hmac}
```

为保证一条安全隧道连接,Easy VPN 不支持提供加密但不提供认证的变换集,也不支持提供认证但不进行加密的变换集。

(6) 创建动态加密图。

```
Router(config)#crypto dynamic-map dynamic-map-name dynamic-map-number
Router(config-crypto-map)#set transform-set transform-set-name
Router(config-crypto-map)#reverse-route
```

其中,reverse-route 命令用来为每一个 VPN 客户端的内部 IP 地址在 Easy VPN 服务器上创建一条静态路由,以保证 IPSec 隧道的返回数据能够找到该隧道。

(7) 配置 VPN 服务器响应客户端请求并为其授权的方案。

```
Router(config)#crypto map map-name client configuration address respond
Router(config)#crypto map map-name client authentication list list-name
Router(config)#crypto map map-name isakmp authorization list list-name
```

(8) 配置加密图。

```
Router(config)#crypto map map-name seq-number ipsec-isakmp dynamic dynamic-map-name
```

动态加密图不能直接应用在接口上,因此需要创建一个静态加密图并将动态加密图插入到静态加密图中。

(9) 将加密图应用到接口上。

```
Router(config-if)#crypto map map-name
```

(10) 启用 IKE 失效对等体检测。

```
Router(config)#crypto isakmp keepalive second
```

2. Easy VPN 客户端配置

使用 Cisco VPN 客户端软件，可以帮助用户连接到 Easy VPN 服务器，建立 IPSec VPN 安全隧道，该软件的主窗口如图 4-59 所示。

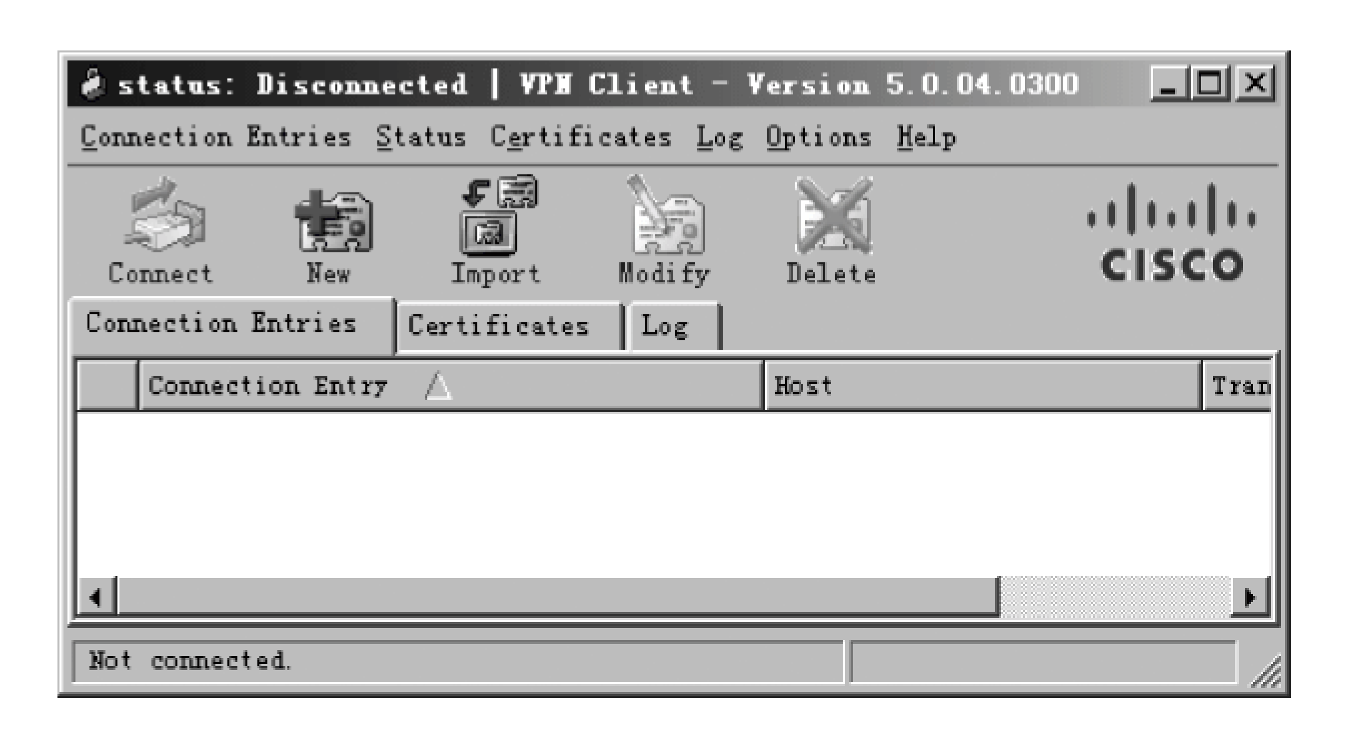


图 4-59　Cisco VPN 客户端软件主窗口

(1) 创建 VPN 连接配置项并定义连接参数。

在主窗口中单击“New”图标新建一个连接配置，出现如图 4-60 所示的“创建新 VPN 连接”窗口，在该窗口中输入 VPN 连接所需参数。

图 4-60　新建 VPN 连接配置窗口

在“创建新 VPN 连接”窗口中，建立预共享密钥方式 VPN 连接所需的必要参数有：VPN 服务器地址 Host、组策略名 Name、组策略预共享密钥 Password 和 Confirm Password。

例如，如果 Easy VPN 服务器的 IP 为 200.100.15.205，在 Easy VPN 服务器上为远程访问用户配置了组策略 rvpn-1，组策略预共享密钥为“123”，则可以设置 Host 为 200.100.15.205，Name 为 rvpn-1，Password 和 Confirm Password 为 123。

配置完成后,单击 Save 按钮保存,则在主窗口中会出现新定义的 VPN 连接项记录。

(2) 建立 VPN 连接。

在保证运行该客户端软件的计算机已能连接到 Internet 的情况下,选择 Cisco VPN 客户端软件窗口中已经配置好的 VPN 连接项,然后单击窗口上方的 Connect 图标,连接 Easy VPN 服务器。

在建立连接过程中,如果协商 ISAKMP 策略通过,则 Cisco VPN 客户端软件会弹出如图 4-61 所示窗口,让用户输入用户名和口令。在该窗口中输入在 Easy VPN 服务器上配置的用户名及口令,单击 OK 按钮,发送用户信息。



图 4-61 用户登录认证窗口

如果通过身份认证,并且客户端能与服务器成功协商建立 IPSec SA,则在主窗口相应连接项前将出现一个图标。此时,在命令行界面下执行 ipconfig 命令可以看到客户端获得了企业内部网络地址。

3. Easy VPN 配置举例

在此依然使用图 4-38 所示的网络进行 Easy VPN 的配置。路由器 RTA 上的具体配置命令如下:

```
RTA(config)#ip local pool pool-rvpn 10.1.2.2 10.1.2.254
RTA(config)#aaa new-model
RTA(config)#aaa authentication login authen-vpn local
RTA(config)#aaa authorization network author-vpn local
RTA(config)#username abc password 123456
RTA(config)#crypto isakmp policy 10
RTA(config-isakmp)#authentication pre-share
RTA(config-isakmp)#encryption 3des
RTA(config-isakmp)#group 2
RTA(config-isakmp)#hash md5
RTA(config-isakmp)#exit
RTA(config)#crypto isakmp client configuration group grp-vpn
RTA(config-isakmp-group)#key 123
RTA(config-isakmp-group)#pool pool-rvpn
RTA(config-isakmp-group)#netmask 255.255.255.0
RTA(config-isakmp-group)#exit
RTA(config)#crypto ipsec transform-set ts-vpn esp-3des esp-md5-hmac
RTA(cfg-crypto-trans)#exit
RTA(config)#crypto dynamic-map dmap-vpn 10
RTA(config-crypto-map)#set transform-set ts-vpn
```

```
RTA(config-crypto-map)#reverse-route
RTA(config-crypto-map)#exit
RTA(config)#crypto map map-vpn client configuration address respond
RTA(config)#crypto map map-vpn client authentication list authen-vpn
RTA(config)#crypto map map-vpn isakmp authorization list author-vpn
RTA(config)#crypto map map-vpn 10 ipsec-isakmp dynamic dmap-vpn
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#crypto map map-vpn
```

配置完成后，在 PC_1 上安装并配置 Easy VPN 客户端软件，连接成功后在 PC_1 的命令行界面下执行 ipconfig 命令可以看到其获得了企业内部地址 10.1.2.2。

4.5　模拟公司网络安全通信配置方案

根据 4.1 节模拟公司网络安全通信需求，可在分支机构 B-1 边界路由器上进行以下配置。

（1）站到站 VPN，其各项参数如表 4-1 所示。

表 4-1　站到站 VPN 配置参数

ISAKMP 策略	变换集参数	加密图参数
优先级：1 加密算法：3DES 散列算法：SHA D-H 算法：2 认证方式：预共享密钥 预共享密钥：随机生成	变换集名：ts-vpn-公司机构代号 封装协议及加密算法：ESP-3DES 封装协议及认证算法：ESP-SHA-HMAC	加密图名：map-vpn 加密图条目序号：公司机构代号

（2）远程访问 VPN，其主要配置参数如表 4-2 所示。

表 4-2　远程访问 VPN 配置参数

ISAKMP 策略	变换集参数	加密图参数
优先级：1 加密算法：3DES 散列算法：SHA D-H 算法：2 认证方式：预共享密钥 预共享密钥：随机生成	变换集名：ts-rvpn 封装协议及加密算法：ESP-3DES 封装协议及认证算法：ESP-SHA-HMAC	加密图名：map-vpn 动态加密图名：dmap-rvpn 加密图条目序号：100

表 4-1 中“公司机构代号”为公司所有机构网络的数字编号。分支机构与公司其他网络对等体间预共享密钥使用随机算法生成，每月更换。

表 4-2 中分别使用 ts-rvpn 作为变换集名、动态加密图名。

4.6 小结

作为一种防止窃听和恶意篡改的技术,VPN通过对数据进行加密和散列来实现数据的机密性、完整性和反拒认功能。本章基于模拟公司网络安全通信的需求,对站到站VPN技术和远程访问VPN技术分别进行了介绍,其中站到站VPN主要介绍了IPSec VPN的实现;远程访问VPN分别对H3C设备上的L2TP VPN的实现和Cisco设备上的Easy VPN的实现进行了介绍。

4.7 习题

1. 按照加密算法工作方式的不同,可以将加密技术分成哪两种?其典型的加密算法分别有哪些?
2. 请简述散列算法的特点。
3. 请简述ESP协议和AH协议的主要区别。
4. IKE协商可以分为哪两个阶段?在进行第一个阶段协商时有哪两种不同的工作模式?
5. L2TP隧道的建立有哪两种模式?分别由谁发起隧道连接?

4.8 实训

4.8.1 站到站VPN配置实训

实验学时:2学时。

每组实验学生人数:3人。

1. 实验目的

掌握基于IPSec的站到站VPN的配置。

2. 实验环境

(1) 安装有TCP/IP协议的Windows系统PC:3台

(2) 路由器:2台

(3) 二层交换机:1台

(4) UTP电缆:6条

(5) Console电缆:3条

保持路由器和交换机均为出厂配置。

3. 实验内容

配置和验证站到站VPN。

4. 实验指导

(1) 按照图4-62所示的网络拓扑结构搭建网络,完成网络连接。

(2) 按照图4-62所示为路由器和PC配置IP地址,在路由器RTA和RTB上配置

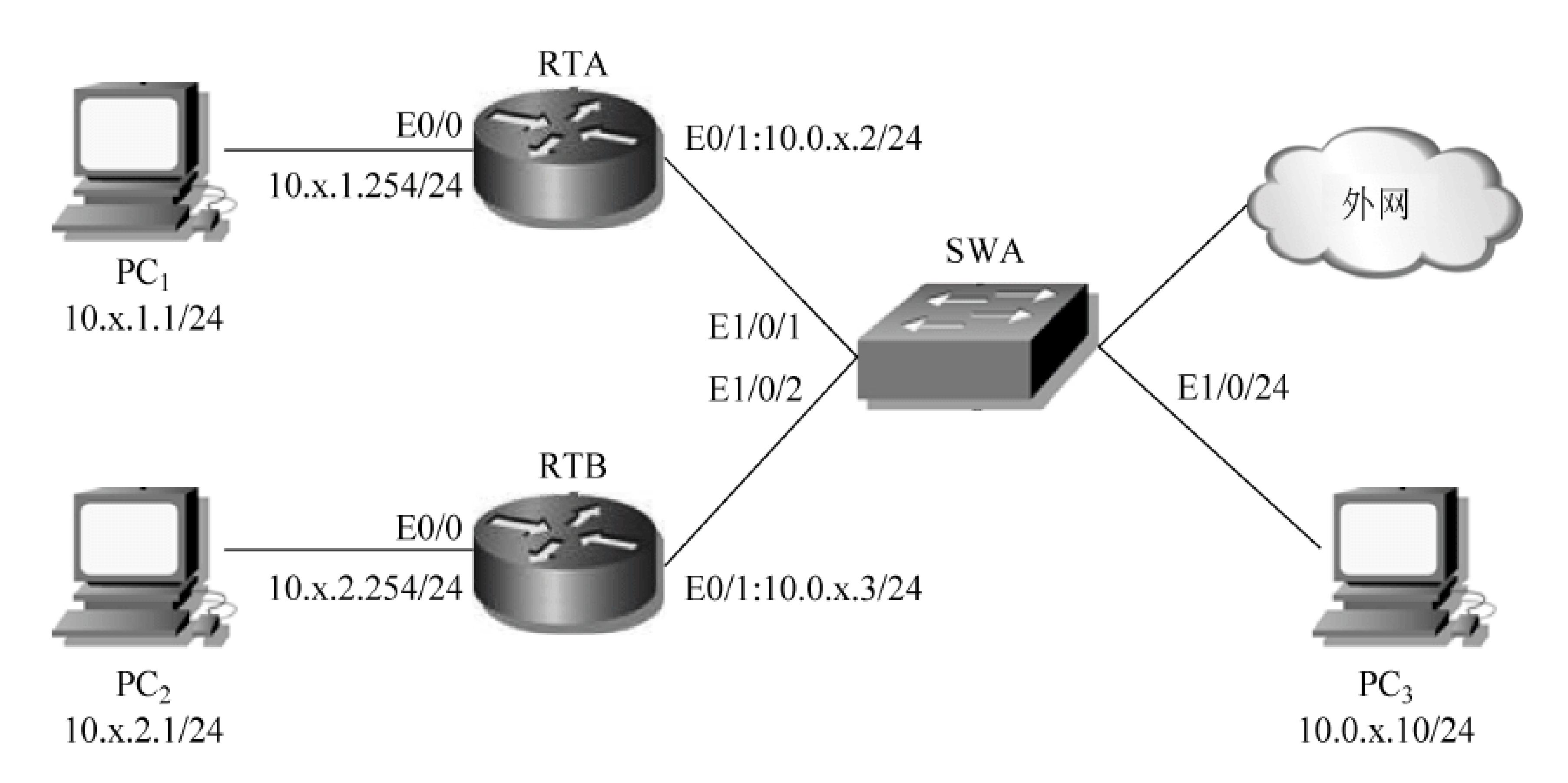


图 4-62　站到站 VPN 配置实训

RIPv2 协议以及配置默认路由,实现整个网络的联通性。

(3) 在交换机 SWA 上配置端口镜像,将端口 E1/0/1 和 E1/0/2 的出入站流量均镜像到端口 E1/0/24 上。

H3C 设备参考命令如下:

```
[SWA]mirroring-group 1 local
[SWA]mirroring-group 1 mirroring-port Ethernet 1/0/1 to Ethernet 1/0/2 both
[SWA]mirroring-group 1 monitor-port Ethernet 1/0/24
```

Cisco 设备参考命令如下:

```
SWA(config)#monitor session 1 source interface FastEthernet 0/1 - 2 both
SWA(config)#monitor session 1 destination interface FastEthernet 0/24
```

(4) 在路由器 RTA 和 RTB 上配置基于 IPSec 的站到站 VPN 来保护 PC_1 和 PC_2 所在网段之间的通信流量。要求对等体身份认证采用预共享密钥的方式,预共享密钥为 123456;IPSec 封装协议采用 AH 协议;其他配置均使用系统默认配置。

H3C 路由器 RTA 上的 IPSec 参考配置如图 4-63 所示。

Cisco 路由器 RTA 上的 IPSec 参考配置命令如下:

```
RTA(config)#crypto isakmp policy 10
RTA(config-isakmp)#authentication pre-share
RTA(config-isakmp)#encryption des
RTA(config-isakmp)#group 1
RTA(config-isakmp)#hash sha
RTA(config-isakmp)#lifetime 86400
RTA(config-isakmp)#exit
RTA(config)#crypto isakmp key 0 123456 address 10.0.x.3
RTA(config)#crypto ipsec transform-set ts-vpn ah-md5-hmac
RTA(cfg-crypto-trans)#exit
RTA(config)#ip access-list extended eacl-vpn
RTA(config-ext-nacl)#permit ip 10.x.1.0 0.0.0.255 10.x.2.0 0.0.0.255
RTA(config-ext-nacl)#exit
```

新建 IPSec 连接

IPSec连接名称 lan-to-lan *字符（1－32）

网关信息

接口 Ethernet0/1

组网模式 ◉站点到站点 ○PC到站点

网关地址

对端网关地址/主机名 10.0.x.3 *字符（1－255）

本端网关地址

认证

认证方式

◉预共享密钥 •••••• *字符（1－128）

○证书

网关ID

对端ID类型 ◉IP地址 ○网关名称

本端ID类型 ◉IP地址 ○网关名称

筛选器

筛选方式 流量特征

源地址/通配符 10.x.1.0 / 0.0.0.255 *

目的地址/通配符 10.x.2.0 / 0.0.0.255 *

▼高级

第一阶段

交换模式 ◉主模式 ○野蛮模式

认证算法 SHA1

加密算法 DES

DH Diffie-Hellman Group1

SA的生存周期 86400 秒（60－604800，缺省值＝86400）

第二阶段

协议 AH

AH认证算法 MD5

封装模式 ◉隧道模式 ○传输模式

PFS None

SA的生存周期

基于时间的生存周期 3600 秒（180－604800，缺省值＝3600）

基于流量的生存周期 1843200 千字节（2560－4294967295，缺省值:

DPD ○开启 ◉关闭

选择加密卡 << >>

星号(*)为必须填写项

确定 取消

图 4-63 路由器 RTA 上 IPSec 配置

```
RTA(config)#crypto map map-vpn 10 ipsec-isakmp
RTA(config-crypto-map)#set peer 10.0.x.3
RTA(config-crypto-map)#set transform-set ts-vpn
RTA(config-crypto-map)#match address eacl-vpn
RTA(config-crypto-map)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#crypto map map-vpn
```

路由器 RTB 上的 IPSec 配置与 RTA 类似，区别是 RTB 上设置的对端网关地址/主机名为 10.0.x.2，基于流量特征的筛选条件与路由器 RTA 完全对称。

(5) 配置完成后，在 PC_1 上使用 ping 命令连接 PC_2，同时在 PC_3 上使用 Wireshark 软件捕获数据报文。查看捕获的数据报文中 IKE 协议两个阶段协商的过程，了解使用主模式进行 ISAKMP SA 协商的 3 对消息的协商内容；查看 AH 封装的数据报文，比较数据报文中内部 IP 报头(原 IP 报头)和外部 IP 报头(新 IP 报头)中源 IP 地址和目的 IP 地址的区别；给出 AH 协议的报文封装结构。

(6) 分别在路由器 RTA 和 RTB 上查看已建立的 IPSec 隧道信息，比较两台路由器上 IPSec 隧道的流量特征和 SPI 是否对称。

5. 实验报告

<table>
<tr><td rowspan="3">RTA</td><td colspan="4">对端网关地址/主机名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="3">源地址/通配符</td><td colspan="4"></td></tr>
<tr><td colspan="3">目的地址/通配符</td><td colspan="4"></td></tr>
<tr><td rowspan="3">RTB</td><td colspan="4">对端网关地址/主机名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="3">源地址/通配符</td><td colspan="4"></td></tr>
<tr><td colspan="3">目的地址/通配符</td><td colspan="4"></td></tr>
<tr><td rowspan="2">ISAKMP SA 协商报文</td><td colspan="2"></td><td colspan="3">第一对消息</td><td colspan="2">第二对消息</td><td>第三对消息</td></tr>
<tr><td colspan="2">Next payload</td><td colspan="3"></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4">AH 报文</td><td colspan="3" rowspan="2">内部 IP 报头</td><td colspan="3">源 IP 地址</td><td colspan="2">目的 IP 地址</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3" rowspan="2">外部 IP 报头</td><td colspan="3">源 IP 地址</td><td colspan="2">目的 IP 地址</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>AH 协议报文封装结构</td><td colspan="8"></td></tr>
<tr><td rowspan="8">IPSec 隧道监控信息</td><td colspan="2" rowspan="4">RTA</td><td colspan="3" rowspan="2">流量特征</td><td colspan="2">src</td><td>dst</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3" rowspan="2">SPI</td><td colspan="2">in</td><td>out</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2" rowspan="4">RTB</td><td colspan="3" rowspan="2">流量特征</td><td colspan="2">src</td><td>dst</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3" rowspan="2">SPI</td><td colspan="2">in</td><td>out</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

4.8.2　远程访问 VPN 配置实训

实验学时：4 学时。

每组实验学生人数：4人。

1. 实验目的

掌握基于(L2TP+IPSec)/Easy VPN的远程访问VPN配置。

2. 实验环境

(1) 安装有TCP/IP协议的Windows系统PC：5台

(2) 路由器：4台

(3) 三层交换机：1台

(4) 二层交换机：1台

(5) UTP电缆：11条

(6) Console电缆：5条

保持路由器和交换机均为出厂配置。

3. 实验内容

配置和验证远程访问VPN。

4. 实验指导

(1) 按照图4-64所示的网络拓扑结构搭建网络，完成网络连接。其中交换机SWA与路由器RTA、RTB、RTC和RTD分别使用接口E1/0/1、E1/0/2、E1/0/3和E10/4相连。

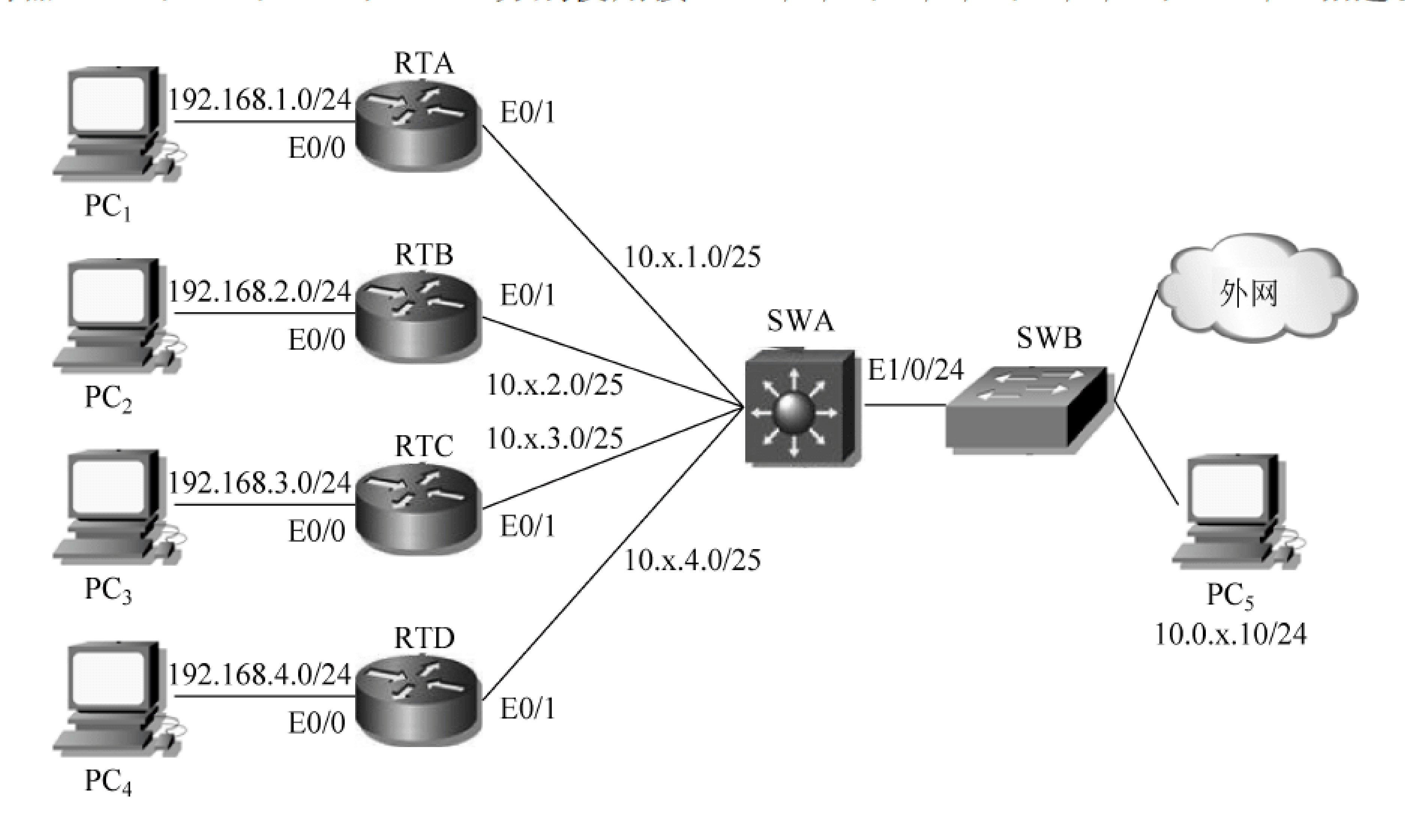


图4-64　远程访问VPN配置实训

(2) 按照图4-64所示为路由器、交换机和PC配置IP地址，其中路由器的E0/0接口使用相应网段中的最后一个可用地址，PC_1～PC_4使用相应网段中的第一个可用地址，路由器的E0/1接口和相连的交换机SWA接口分别使用相应网段的前两个可用地址，PC_5的网关地址设置为交换机SWA的接口E1/0/24的IP地址10.0.x.2。在4台路由器和交换机SWA上仅配置默认路由保障整个网络的联通性。

H3C设备参考命令如下：

```
[RTA]interface Ethernet 0/0
[RTA-Ethernet0/0]ip address 192.168.1.254 24
[RTA-Ethernet0/0]quit
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]ip address 10.x.1.1 25
[RTA-Ethernet0/0]quit
[RTA]ip route-static 0.0.0.0 0 10.x.1.2
--------其他 3 台路由器配置略--------

[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port link-mode route
[SWA-Ethernet1/0/1]ip address 10.x.1.2 25
[SWA-Ethernet1/0/1]quit
--------接口 Ethernet 1/0/2、Ethernet 1/0/3、Ethernet 1/0/4 配置略--------
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-mode route
[SWA-Ethernet1/0/24]ip address 10.0.x.2 24
[SWA-Ethernet1/0/24]quit
[SWA]ip route-static 0.0.0.0 0 10.0.x.1
```

Cisco 设备参考命令如下：

```
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip address 192.168.1.254 255.255.255.0
RTA(config-if)#no shutdown
RTA(config-if)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip address 10.x.1.1 255.255.255.128
RTA(config-if)#no shutdown
RTA(config-if)#exit
RTA(config)#ip route 0.0.0.0 0.0.0.0 10.x.1.2
--------其他 3 台路由器配置略--------

SWA(config)#interface FastEthernet 0/1
SWA(config-if)#no switchport
SWA(config-if)#ip address 10.x.1.2 255.255.255.128
SWA(config-if)#exit
--------接口 FastEthernet 0/2、FastEthernet 0/3、FastEthernet 0/4 配置略--------
SWA(config)#interface FastEthernet 0/24
SWA(config-if)#no switchport
SWA(config-if)#ip address 10.0.x.2 255.255.255.0
SWA(config-if)#exit
SWA(config)#ip routing
SWA(config)#ip route 0.0.0.0 0.0.0.0 10.0.x.1
```

配置完成后，在 4 台路由器上使用 ping 命令测试与外部网络的联通性，应该可以 ping 通。但需要注意此时 PC_1～PC_4 均无法联通外部网络，因为交换机 SWA 并不知道 PC 所在网段的存在。在本实验中 PC_1～PC_4 模拟远程用户，4 台路由器分别扮演 4 个 LNS 的角色，而路由器的 E0/1 接口连接的部分(包括外网网云)作为企业内部网络出现。

本实验希望通过为 PC_1～PC_4 分配企业内部网络地址，使其可以访问企业内部网络(实际上就是 PC_5 以及外网网云部分)。

(3) 配置 L2TP+IPSec VPN 或者 Easy VPN，使 PC_1～PC_4 可以通过 L2TP+IPSec 隧道或者 Easy VPN 隧道访问企业内部网络。其中 L2TP 中 PPP 认证方式采用 CHAP，用户名和密码均分别是 network 和 123456；为远程用户分配的 IP 地址段分别为 10.x.1.128/25、10.x.2.128/25、10.x.3.128/25 和 10.x.4.128/25。IPSec 对等体身份认证使用的预共享密钥均为 abc。

首先在三层交换机 SWA 上配置去往为远程用户分配的 4 个网段的路由，确保远程用户通过远程访问 VPN 连接可以访问企业内部网络。

H3C 设备参考命令如下：

```
[SWA]ip route-static 10.x.1.128 25 10.x.1.1
[SWA]ip route-static 10.x.2.128 25 10.x.2.1
[SWA]ip route-static 10.x.3.128 25 10.x.3.1
[SWA]ip route-static 10.x.4.128 25 10.x.4.1
```

Cisco 设备参考命令如下：

```
SWA(config)#ip route 10.x.1.128 255.255.255.128 10.x.1.1
SWA(config)#ip route 10.x.2.128 255.255.255.128 10.x.2.1
SWA(config)#ip route 10.x.3.128 255.255.255.128 10.x.3.1
SWA(config)#ip route 10.x.4.128 255.255.255.128 10.x.4.1
```

H3C 路由器 RTA 上 L2TP+IPSec VPN 的参考配置如图 4-65～图 4-67 所示。注意在配置之前先将 PC_1 的公网 IP 地址修改为 192.168.1.0/24 网段的另外一个地址，然后再登录路由器 RTA 进行配置，以避免配置 IPSec 后无法登录路由器 RTA。

其中，L2TP 配置中的修改 ISP 域配置和创建新用户的配置图略。

将 PC_1 的公网 IP 地址修改回 192.168.1.1，然后在 PC_1 上启动 IPSec Services 服务并创建虚拟专用网络连接，具体的配置请参考 4.4.1 小节的相关内容。

Cisco 路由器 RTA 上 Easy VPN 的配置参考命令如下：

```
RTA(config)#ip local pool pool-rvpn 10.x.1.130 10.x.1.254
RTA(config)#aaa new-model
RTA(config)#aaa authentication login authen-vpn local
RTA(config)#aaa authorization network author-vpn local
RTA(config)#username network password 123456
RTA(config)#crypto isakmp policy 10
RTA(config-isakmp)#authentication pre-share
RTA(config-isakmp)#encryption 3des
RTA(config-isakmp)#group 2
RTA(config-isakmp)#hash md5
RTA(config-isakmp)#exit
RTA(config)#crypto isakmp client configuration group grp-vpn
RTA(config-isakmp-group)#key abc
RTA(config-isakmp-group)#pool pool-rvpn
RTA(config-isakmp-group)#netmask 255.255.255.128
```

新建IPSec连接

IPSec连接名称　l2tp+ipsec　* 字符（1－32）

网关信息

接口　Ethernet0/0

组网模式　⦿ 站点到站点 ○ PC到站点

网关地址

对端网关地址/主机名　192.168.1.1　* 字符（1－255）

本端网关地址

认证

认证方式

⦿ 预共享密钥　●●●　* 字符（1－128）

○ 证书

网关ID

对端ID类型　⦿ IP地址 ○ 网关名称

本端ID类型　⦿ IP地址 ○ 网关名称

筛选器

筛选方式　流量特征

源地址/通配符　0.0.0.0　/255.255.255.255　*

目的地址/通配符　192.168.1.1　/0.0.0.0　*

▼高级

第一阶段

交换模式　⦿ 主模式 ○ 野蛮模式

认证算法　SHA1

加密算法　DES

DH　Diffie-Hellman Group1

SA的生存周期　86400　秒（60－604800，缺省值＝86400）

第二阶段

协议　ESP

ESP认证算法　MD5

ESP加密算法　3DES

封装模式　○ 隧道模式 ⦿ 传输模式

PFS　None

SA的生存周期

基于时间的生存周期　3600　秒（180－604800，缺省值＝3600）

基于流量的生存周期　250000　千字节（2560－4294967295，缺省值＝1843200）

DPD　○ 开启 ⦿ 关闭

选择加密卡　<<　>>

星号（*）为必须填写项

确定　取消

图 4-65　路由器 RTA 上 IPSec 配置

新建L2TP用户组	
L2TP配置	
L2TP用户组名称：	l2tp+ipsec *字符(1-15)
对端隧道名称：	字符(1-30)
本端隧道名称：	字符(1-30)
隧道验证：	禁用
隧道验证密码：	字符(1-16)
PPP认证配置	
PPP认证方式：	CHAP
ISP域名：	system 新建 修改 删除
PPP地址配置	
PPP Server 地址/掩码：	10.x.1.129 / 255.255.255.128 *
用户地址：	新建 修改 删除 强制分配地址：禁用
□高级	
星号(*)为必须填写项	

图 4-66 路由器 RTA 上 L2TP 配置

新建地址池	
域名：	system
地址池编号：	1 *(0-99)
开始地址：	10.x.1.130 *
结束地址：	10.x.1.254
星号(*)为必须填写项	
确定 取消	

图 4-67 路由器 RTA 上创建为远程用户分配地址的地址池

```
RTA(config-isakmp-group)#exit
RTA(config)#crypto ipsec transform-set ts-vpn esp-3des esp-md5-hmac
RTA(cfg-crypto-trans)#exit
RTA(config)#crypto dynamic-map dmap-vpn 10
RTA(config-crypto-map)#set transform-set ts-vpn
RTA(config-crypto-map)#reverse-route
RTA(config-crypto-map)#exit
RTA(config)#crypto map map-vpn client configuration address respond
RTA(config)#crypto map map-vpn client authentication list authen-vpn
RTA(config)#crypto map map-vpn isakmp authorization list author-vpn
RTA(config)#crypto map map-vpn 10 ipsec-isakmp dynamic dmap-vpn
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#crypto map map-vpn
```

Easy VPN 客户端的配置请参考 4.4.2 小节的相关内容。

路由器 RTB、RTC 和 RTD 上的配置与路由器 RTA 上的配置类似，PC_2、PC_3 和 PC_4 上的配置和 PC_1 类似，在此不再赘述。

配置完成后，使用 PC_1～PC_4 上新建的虚拟专用网连接与相对应的路由器之间建立 L2TP＋IPSec 的隧道连接。建立连接后，在命令行模式下使用 ipconfig 命令查看 PC 获得的企业内部网络 IP 地址；在路由器上查看已建立的 IPSec 隧道信息和 L2TP 隧道信息。

在 PC_1～PC_4 上使用 ping 命令连接 PC_5，同时在通信两端的 PC 上分别使用 Wireshark 软件捕获数据报文。比较在远程 PC 上捕获的数据报文中的源 IP 地址和目的 IP 地址与在 PC_5 上捕获的数据报文中的源 IP 地址和目的 IP 地址的区别，H3C 设备结合图 4-58 对其进行分析。

在 PC_1～PC_4 上使用 ping 命令测试到达外网网云中的某站点的联通性，例如百度网站。可以 ping 通，分析其原因（**注意**：网络综合实验室的出口路由器上没有设置 192.168.0.0/16 网段的地址转换，也就是说对于源 IP 地址属于 192.168.0.0/16 网段的数据报文无法连接 Internet）。

5. 实验报告

<table>
<tr><td rowspan="7">RTA 上 L2TP＋IPSec VPN 的配置</td><td colspan="3">对端网关地址/主机名</td><td colspan="3"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="2">源地址/通配符</td><td colspan="3"></td></tr>
<tr><td colspan="2">目的地址/通配符</td><td colspan="3"></td></tr>
<tr><td>封装模式</td><td colspan="2"></td><td colspan="2">基于流量的生存周期</td><td></td></tr>
<tr><td colspan="3">PPP Server 地址/掩码</td><td colspan="3"></td></tr>
<tr><td colspan="2" rowspan="2">为远程用户分配地址的地址池</td><td colspan="2">开始地址</td><td colspan="2">结束地址</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>RTA 上 Easy VPN 的配置</td><td colspan="6"></td></tr>
<tr><td rowspan="7">RTB 上 L2TP＋IPSec VPN 的配置</td><td colspan="3">对端网关地址/主机名</td><td colspan="3"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="2">源地址/通配符</td><td colspan="3"></td></tr>
<tr><td colspan="2">目的地址/通配符</td><td colspan="3"></td></tr>
<tr><td>封装模式</td><td colspan="2"></td><td colspan="2">基于流量的生存周期</td><td></td></tr>
<tr><td colspan="3">PPP Server 地址/掩码</td><td colspan="3"></td></tr>
<tr><td colspan="2" rowspan="2">为远程用户分配地址的地址池</td><td colspan="2">开始地址</td><td colspan="2">结束地址</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>RTB 上 Easy VPN 的配置</td><td colspan="6"></td></tr>
<tr><td rowspan="7">RTC 上 L2TP＋IPSec VPN 的配置</td><td colspan="3">对端网关地址/主机名</td><td colspan="3"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="2">源地址/通配符</td><td colspan="3"></td></tr>
<tr><td colspan="2">目的地址/通配符</td><td colspan="3"></td></tr>
<tr><td>封装模式</td><td colspan="2"></td><td colspan="2">基于流量的生存周期</td><td></td></tr>
<tr><td colspan="3">PPP Server 地址/掩码</td><td colspan="3"></td></tr>
<tr><td colspan="2" rowspan="2">为远程用户分配地址的地址池</td><td colspan="2">开始地址</td><td colspan="2">结束地址</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>RTC 上 Easy VPN 的配置</td><td colspan="6"></td></tr>
</table>

续表

<table>
<tr><td rowspan="7">RTD 上 L2TP＋IPSec VPN 的配置</td><td colspan="4">对端网关地址/主机名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">筛选器</td><td colspan="3">源地址/通配符</td><td colspan="4"></td></tr>
<tr><td colspan="3">目的地址/通配符</td><td colspan="4"></td></tr>
<tr><td>封装模式</td><td colspan="3"></td><td colspan="3">基于流量的生存周期</td><td></td></tr>
<tr><td colspan="4">PPP Server 地址/掩码</td><td colspan="4"></td></tr>
<tr><td colspan="3" rowspan="2">为远程用户分配地址的地址池</td><td colspan="3">开始地址</td><td colspan="2">结束地址</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>RTD 上 Easy VPN 的配置</td><td colspan="8"></td></tr>
<tr><td rowspan="6">Wireshark 报文分析</td><td colspan="2"></td><td colspan="3">源 IP 地址</td><td colspan="3">目的 IP 地址</td></tr>
<tr><td colspan="2">PC_1</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="2">PC_2</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="2">PC_3</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="2">PC_4</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="2">PC_5</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>PC_1 至 PC_4 可以 ping 通 Internet 网络站点的原因</td><td colspan="8"></td></tr>
</table>

第 5 章

防　火　墙

本章任务：根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题。

必备知识：(1) 防火墙工作原理。

(2) 防火墙网络联通性配置。

(3) 防火墙域间策略配置。

学习目标：完成模拟公司网络边界防火墙的安全配置，防御来自 Internet 的安全威胁。

5.1　模拟公司总部网络内外网边界安全任务分析

模拟公司总部网络安全通信需求如下：

(1) 模拟公司总部 Web 服务器、邮件服务器需对外提供 24h 服务。

(2) 模拟公司总部网络内主机可以访问 Internet 上各种资源，但非公司所属机构的外部网络主机，不能主动连接模拟公司总部网络内主机。

以上安全通信需求虽然可以使用配置了 ACL 的路由器来实现，但路由器的主要功能是进行数据转发和路由，当网络流量较大时，难以保障网络性能。为解决网络安全与性能间的矛盾，模拟公司总部网络选择在网络边界上配置硬件防火墙来完成网络通信过滤等安全功能。为满足总部网络的安全通信需求，防火墙上需要进行如下配置：

(1) 基本网络联通性配置。

(2) 配置域间策略，允许外部网络访问内部 Web、邮件服务。

(3) 配置域间策略，允许外部网络对内部网络已建立连接的访问，但禁止所有其他的 TCP 连接。

5.2　防火墙基础知识

防火墙实际上就是可以在两个或多个网络间实施访问控制策略的一个或一组系统。根据实现方式的区别，防火墙可以分为以下 3 种类型。

(1) 基于服务器的防火墙。基于服务器的防火墙是基于 Windows、Unix 等操作系统

的防火墙应用,即软件防火墙,例如瑞星防火墙、天网防火墙等。软件防火墙一般只能保护一台主机,而且软件防火墙需要使用安装宿主机的系统资源来实现安全防护,性能相对较低,在处理较大数据流量时甚至可能拖垮宿主机。另外软件防火墙无法对宿主机操作系统本身存在的缺陷进行安全防护。

(2) 集成防火墙。集成防火墙是指在已存在的设备上增加防火墙功能。比较典型的是在路由器或者三层交换机上集成防火墙的部分功能。

(3) 基于设备的防火墙。基于设备的防火墙即专门的硬件防火墙,硬件防火墙专为实现网络安全策略而设计,硬件以及内置的操作系统专门针对数据过滤进行了优化,可以在尽量不影响网络性能的情况下提供网络安全保障。

本章主要对基于设备的防火墙进行介绍。

5.2.1 防火墙的安全区域和安全级别

与路由器在默认情况下允许所有的数据流量不同,作为专门的网络安全设备,防火墙在默认情况下以其接口为边界将网络划分成若干个安全区域,并为其赋予不同的安全级别以控制不同安全区域之间的访问。典型的防火墙安全区域划分如图5-1所示。

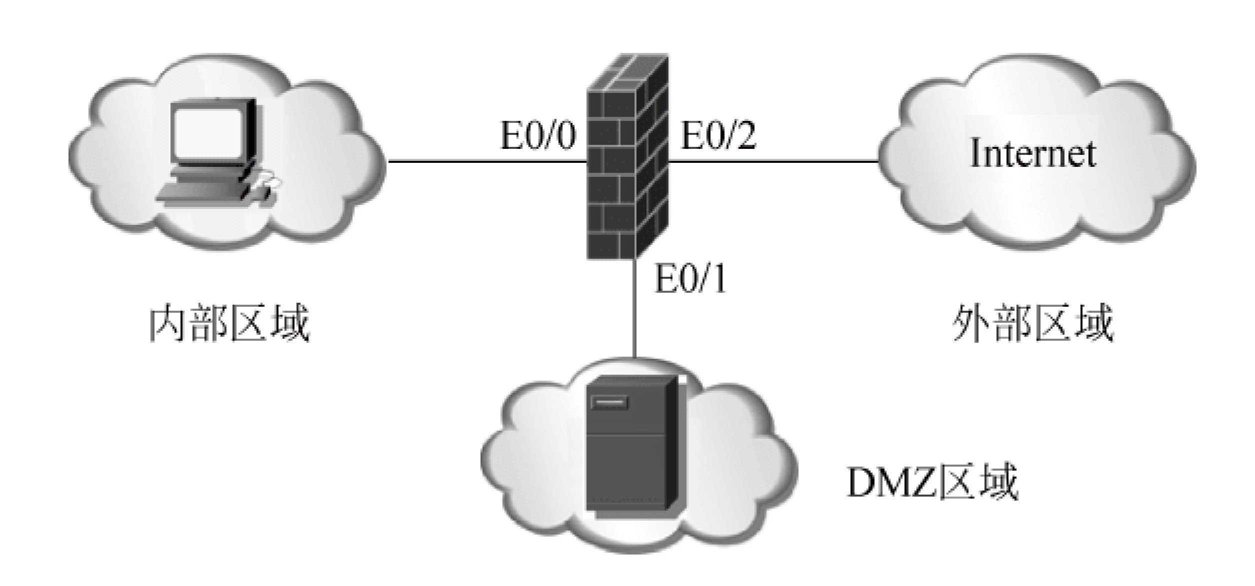


图5-1 防火墙的安全区域划分

1. 内部区域

内部区域又称为Trust区域,该区域连接的是企业内部网络,该区域为受信任区域,受到防火墙的保护。该区域一般被赋予较高的安全级别,对于Cisco的PIX系列防火墙而言,为连接内部区域的inside接口设置最高的安全级别100;对于H3C的防火墙而言,为Trust区域设置的安全级别为85。

注意: Cisco防火墙的安全级别是针对接口设置的,而H3C防火墙的安全级别是针对安全区域设置的。

在传统上,防火墙的安全级别以及安全策略配置均围绕接口进行,即为具体的物理接口配置不同的安全级别,并在接口之间设置安全策略。随着防火墙设备可以提供的物理接口数量增多,传统基于接口的安全策略配置方式配置和维护的工作量成倍增加,因此部分厂商开始围绕安全区域设置安全级别和安全策略。通过将安全需求相同的接口划分到同一个安全区域中,然后在安全区域间设置安全策略,实现了安全策略的分层管理,简化了安全策略维护的复杂度,同时也实现了网络业务和安全业务的分离。但是在网络复杂度不高的场合,一般还是建议为每一个物理接口单独设置不同的安全区域,以保证域间安全策略配置的灵活性。

2. 外部区域

外部区域又称为 Untrust 区域，该区域连接的是 Internet 等外部网络，该区域是不被信任的区域，位于该区域中的主机访问其他区域主机时将受到严格的安全策略限制。该区域一般被赋予最低的安全级别，对于 Cisco 的 PIX 系列防火墙而言，为连接外部区域的 outside 接口设置最低的安全级别 0；对于 H3C 的防火墙而言，为 Untrust 区域设置的安全级别为 5。

3. DMZ 区域

DMZ 区域即非军事化区域（Demilitarized Zone），它是一个物理上和逻辑上均与内部网络和外部网络相隔离的区域。一般在该区域内放置需要被外部网络访问的 Web 服务器、FTP 服务器等应用服务器，位于 DMZ 区域内的主机或服务器被称为堡垒主机。该区域一般被赋予介于内部区域和外部区域之间的安全级别，对于 Cisco 的 PIX 系列防火墙而言，为连接 DMZ 区域的接口设置最低的安全级别 0；对于 H3C 的防火墙而言，为 DMZ 区域设置的安全级别为 50。

通过设置 DMZ 区域，将企业内部对外提供服务的服务器和普通主机隔离开，在对外提供服务的同时有效保护了企业内部网络中普通主机的安全。

H3C 的防火墙除了 Trust、Untrust 和 DMZ 3 个安全区域以外，还存在两个比较特殊的安全区域：Management 区域和 Local 区域，这两个区域的安全级别均为最高值 100。其中 Management 区域为管理区域，默认情况下，防火墙的第一个接口处于 Management 区域中，Management 区域专门用来通过 Web 对防火墙进行配置管理，Management 区域并不属于业务安全区域。防火墙上除属于 Management 区域接口外的其他所有接口均属于 Local 区域，将某个接口划分到某个特定的区域中只是意味着该接口下所连接的网络属于某个特定的区域，而接口本身只属于 Local 区域，不会发生改变。因此，对于 H3C 的防火墙，其在实际的网络应用中真正进行业务网络安全访问控制的依然是 Trust、Untrust 和 DMZ 3 个安全区域。H3C 防火墙的安全区域划分如图 5-2 所示。

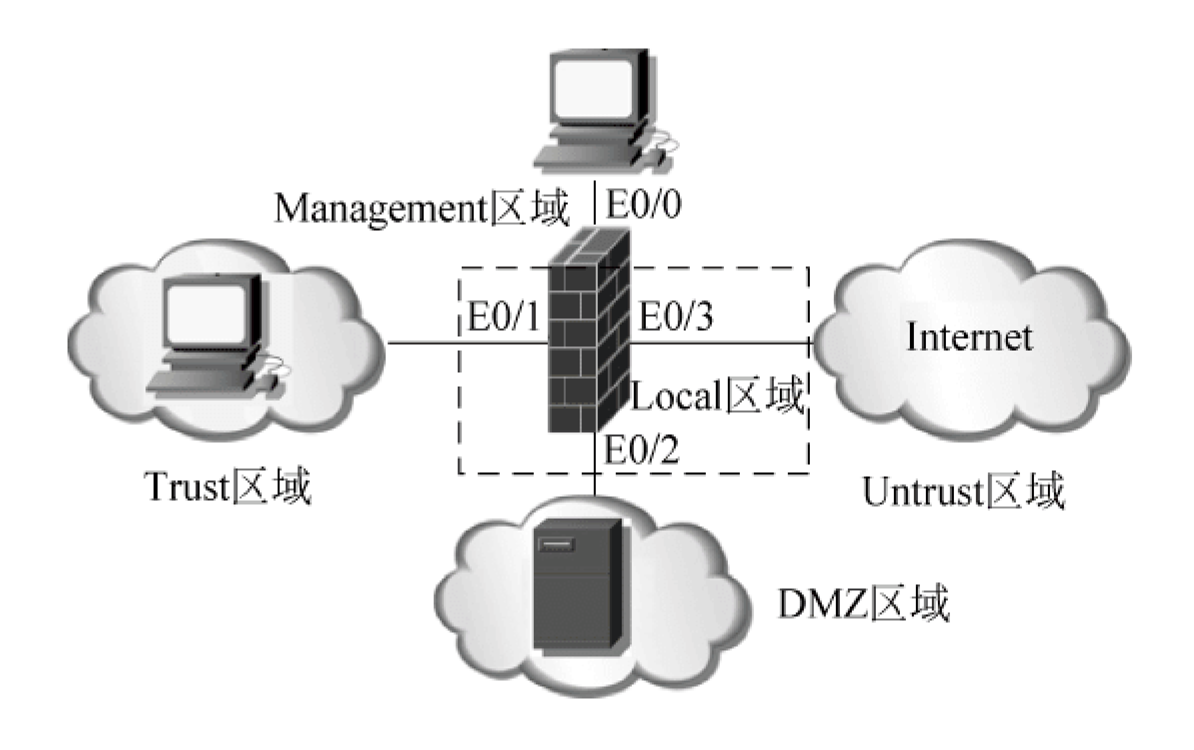


图 5-2　H3C 防火墙的安全区域划分

无论是 Cisco 的防火墙还是 H3C 的防火墙，其默认域间安全策略相同，均为高安全级别的区域能够访问低安全级别的区域，低安全级别的区域不能访问高安全级别的区域。但 H3C 防火墙上的 Local 区域相对比较特殊，虽然 Local 区域拥有最高的安全级别 100，

但默认情况下 Local 区域能够访问其他区域,其他区域也能够访问 Local 区域,这就可以保证无论主机处于哪一个区域均可以保持与防火墙本身的联通性。

5.2.2 防火墙的应用位置

防火墙的典型应用位置如图 5-3 所示。

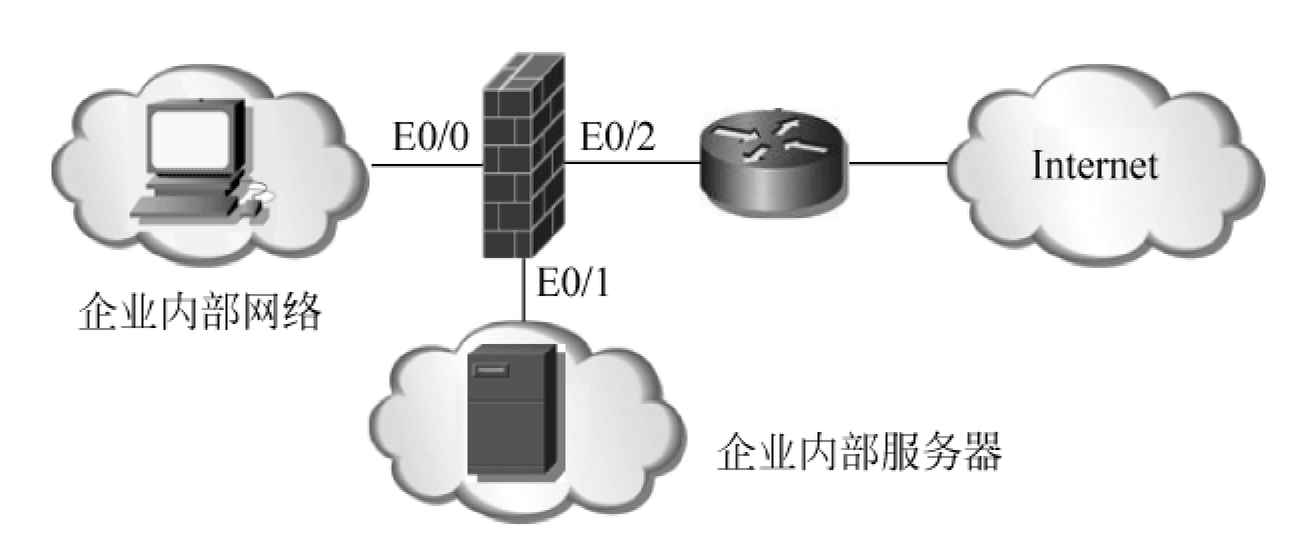


图 5-3 防火墙应用位置 1

从图 5-3 中可以看到,防火墙被放置在接入路由器的后面,由接入路由器实现内外网之间的路由,而防火墙主要用来实现安全访问控制。之所以采用这种方式进行连接,主要考虑以下两点。

(1) 企业局域网络接入到 Internet 中往往使用 SDH、ATM 等广域网链路来实现,路由器可以使用相应的接口模块与其连接,并且实现底层协议的转换,而防火墙只能提供以太网接口,无法实现异构网络之间的连接。

(2) 路由器的路由功能相对更加强大,可以支持多种动态路由选择协议,并且路由性能更佳。传统上防火墙对动态路由选择协议的支持相对较少,并且路由性能相对比较差,如果使用防火墙进行路由很可能成为网络通信中的瓶颈。

但是网络中多串联一个设备,就会多一个潜在故障点,也就会多一个影响网络性能的节点。目前的防火墙设备都能对 RIPv2、OSPF 等动态路由协议提供很好的支持,因此在使用以太网链路接入到 Internet 的应用场合中,往往直接使用一台防火墙来连接 Internet,而不再使用路由器,具体如图 5-4 所示。

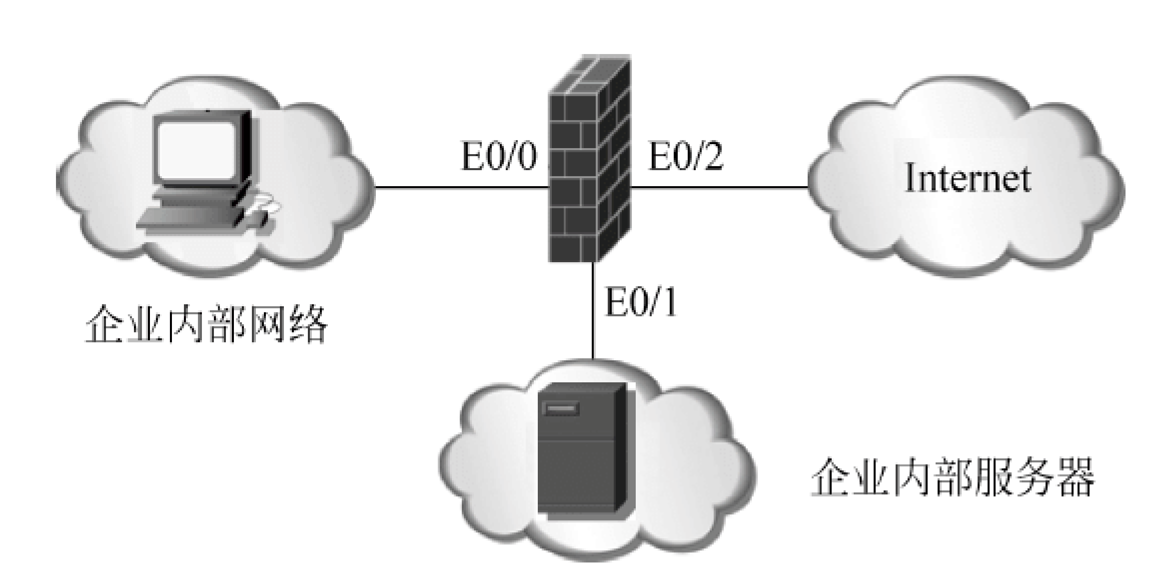


图 5-4 防火墙应用位置 2

实际上,随着技术的不断发展和设备的不断更新,路由器和防火墙之间的功能定位也越来越模糊,一方面路由器能够支持的安全功能不断增加;另一方面防火墙能够支持的路由功能也得到不断的增强。因此在实际的网络应用中,很多时候单独使用路由器或者单独使用防火墙均可以实现用户的路由需求和安全需求。但是路由器的主要功能依然是

实现不同网段之间的路由，而防火墙的主要功能依然是进行网络安全访问控制，其他的功能只是其附属功能。因此在规划网络时，具体是使用路由器还是使用防火墙，或是同时使用两个设备，需要取决于网络的路由需求和安全需求。

5.3 防火墙的配置

5.3.1 H3C 设备配置

在这里以 H3C SecPath U200-CA 为例介绍防火墙的配置。H3C SecPath U200-CA 并不是一台单纯的防火墙设备，而是一款统一威胁管理(United Threat Management，UTM)设备。它在提供传统防火墙、VPN 功能基础上，还提供病毒防护、URL 过滤、漏洞攻击防护、垃圾邮件防护、P2P/IM 应用层流量控制和用户行为审计等安全功能。由于 UTM 设备综合了多项安全功能并且易于管理，目前正逐渐代替传统的防火墙成为主流的信息安全产品。在本章只对 H3C SecPath U200-CA 上的防火墙部分功能进行配置介绍。

H3C SecPath U200-CA 支持命令行配置和 Web 配置两种配置方式，一般推荐在命令行下进行诸如接口 IP 地址等简单的配置以及信息查看、故障诊断等，而在 Web 下进行具体的域间策略等安全配置。

H3C SecPath U200-CA 有 6 个千兆以太口，其中默认 GigabitEthernet0/0 接口处于 Management 区域中，其 IP 地址为 192. 168. 0. 1/24，因此可以使用 IE 通过 GigabitEthernet0/0 接口的 IP 地址登录到 U200-CA 上，默认用户名和密码均为 admin。

防火墙有 3 种不同的工作模式：透明模式、路由模式和混合模式。下面分别对这 3 种不同的工作模式进行配置和介绍。

1. 透明模式的配置

透明(Transparent)模式又称为桥模式，在透明模式下，防火墙的接口均工作在数据链路层，不需要配置 IP 地址。透明模式适用于在已有的网络中增加防火墙设备，这样就可以在不改变原有网络路由的情况下增加防火墙，实现对网络的安全防护。在透明模式下，防火墙多个接口连接的网络属于同一个网段。

假设存在如图 5-5 所示的网络，要求配置防火墙工作在透明模式，其中 PC_1 处于 Trust 区域，PC_2 处于 Untrust 区域。

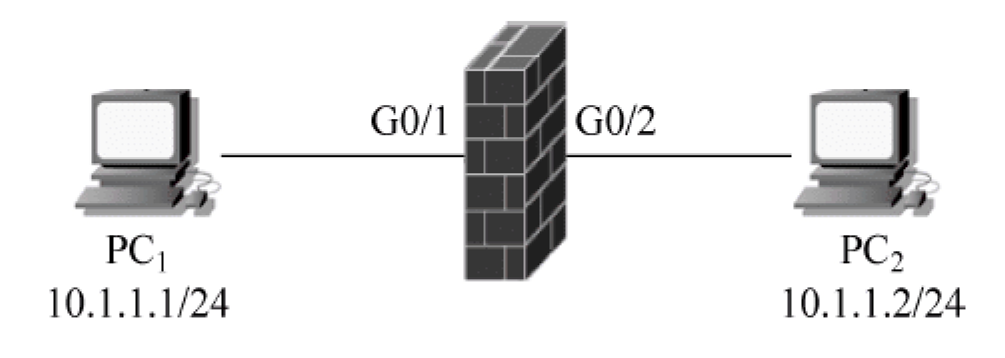


图 5-5 透明模式配置

在默认情况下，防火墙的所有接口均工作在路由模式下，因此首先需要将接口 GigabitEthernet0/1 和 GigabitEthernet0/2 配置为桥模式，并将其划分到同一个 VLAN

中。然后通过 IE 登录到防火墙上,在管理平台界面左侧的导航栏中选择“设备管理>安全域”,进入安全域管理界面,如图 5-6 所示。

安全域ID	安全域名	优先级	共享	虚拟设备	操作
0	Management	100	no	--	
1	Local	100	no	Root	
2	Trust	85	no	Root	
3	DMZ	50	no	Root	
4	Untrust	5	no	Root	

新建

图 5-6　安全域管理界面

单击 Trust 域右侧“操作”字段下的“编辑安全域”图标,进入修改安全域界面,将接口 GigabitEthernet0/1 加入到该域,如图 5-7 所示。

修改安全域

ID: 2

域名: Trust

优先级: 85 (1- 100)

共享: No

虚拟设备: Root

接口: 查询项: 接口 关键字: 查询

	接口	所属VLAN
☐	GigabitEthernet0/3	
☐	GigabitEthernet0/4	
☐	GigabitEthernet0/5	
☐	NULL0	
☑	GigabitEthernet0/1	1-4094
☐	GigabitEthernet0/2	1-4094

所输入的VLAN范围应以“,”及“-”连接,例如:3,5-10

星号(*)为必须填写项

确定　取消

图 5-7　将接口 GigabitEthernet0/1 加入到 Trust 域

同样将接口 GigabitEthernet0/2 加入到 Untrust 域。需要注意的是,将接口 GigabitEthernet0/1 和 GigabitEthernet0/2 加入到 Trust 域和 Untrust 域,只是将相应接口下所连接的网络加入到了 Trust 域和 Untrust 域,GigabitEthernet0/1 和 GigabitEthernet0/2 依然属于 Local 域。

配置完成后,使用 ping 命令进行测试,PC_1 可以 ping 通 PC_2,但 PC_2 无法 ping 通 PC_1,这是因为 PC_2 处于低安全级别的 Untrust 域中,无法访问处于高安全级别的 Trust 域中的 PC_1。如果要实现 PC_2 对 PC_1 的访问,就需要配置域间策略。

除了上面例子中介绍的普通二层转发外,透明模式中还包括 Inline 转发和跨 VLAN 二层转发,具体的配置在此不再进行介绍,感兴趣的同学可以自行查阅相关资料。

2. 路由模式的配置

在路由模式下，防火墙的接口均工作在网络层，不同的接口连接不同的网段，由防火墙来实现不同网段之间的路由。路由模式适用于在新建网络中作为网络接入设备的防火墙。典型的处于路由模式下的防火墙如图 5-8 所示，其中，GigabitEthernet0/1 连接网段 10.1.1.0/24，属于 Trust 域，GigabitEthernet0/2 连接网段 10.1.2.0/24，属于 DMZ 域，GigabitEthernet0/3 连接网段 202.207.127.0/24，属于 Untrust 域。

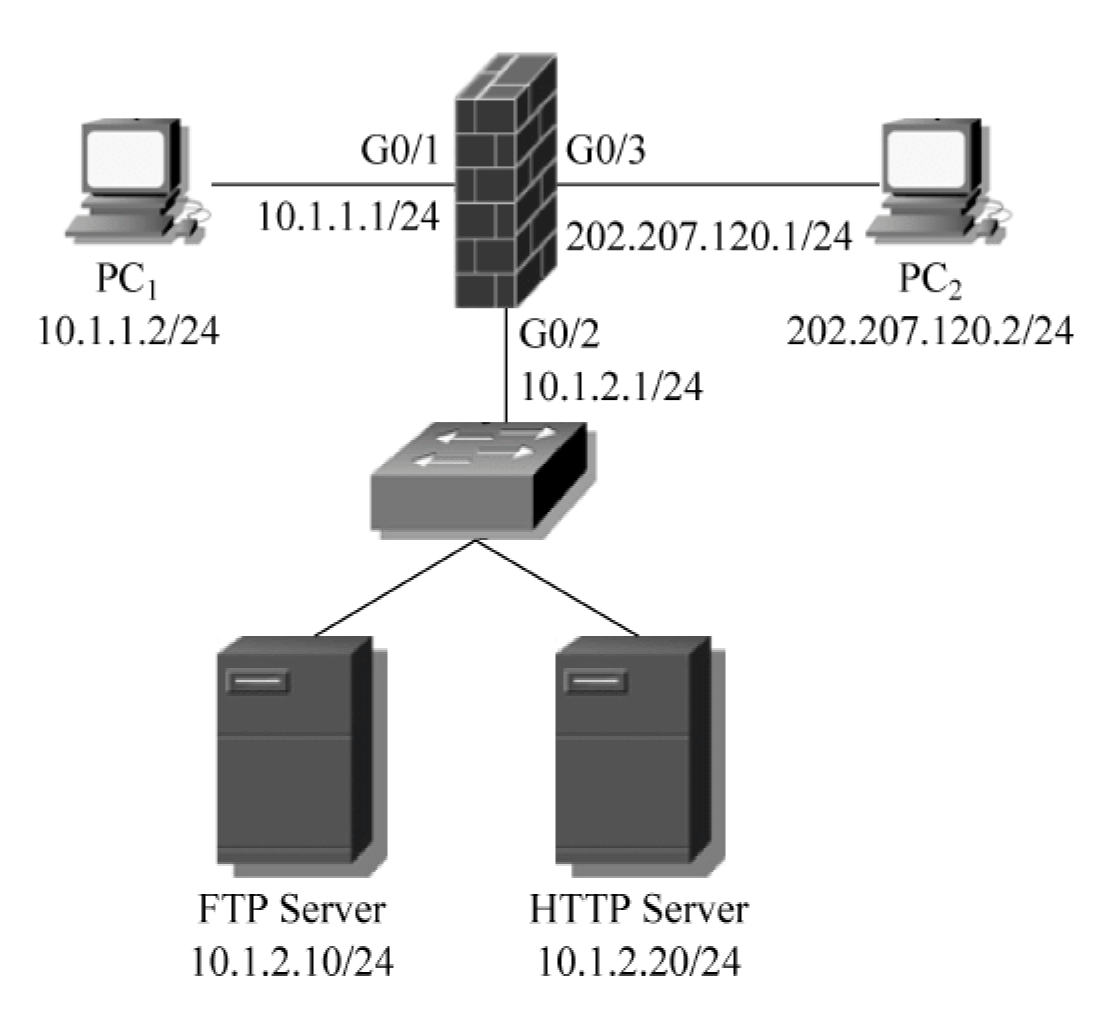


图 5-8　路由模式配置

首先为 GigabitEthernet0/1、GigabitEthernet0/2 和 GigabitEthernet0/3 3 个接口配置 IP 地址，并将其加入到相应的安全区域中。配置完成后，PC_1 可以访问 FTP Server、HTTP Server 和 PC_2；FTP Server 和 HTTP Server 可以访问 PC_2，但不能访问 PC_1；PC_2 无法访问 FTP Server、HTTP Server 和 PC_1。

（1）域间策略配置

在实际的网络应用中，一般需要允许外部网络访问企业内部的服务器，即允许 Untrust 域中的主机访问 DMZ 域中的 FTP Server 和 HTTP Server。为实现这一目的，就需要配置相应的域间策略。在管理平台界面左侧的导航栏中选择“防火墙＞安全策略＞域间策略”，进入域间策略管理界面，如图 5-9 所示。

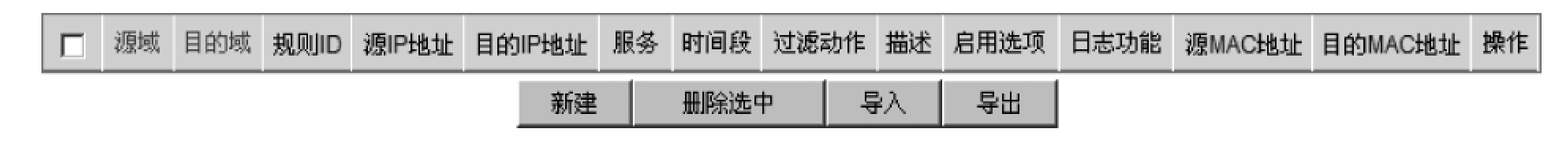


图 5-9　域间策略管理界面

在域间策略管理界面上单击“新建”按钮，进入新建域间策略规则界面，如图 5-10 所示。

首先，新建一条规则允许 Untrust 域中的主机访问 DMZ 域中的 FTP Server。其中



图 5-10　新建域间策略规则界面

参数的解释和设置如下。

① 源域：设置域间策略规则的源区域，在此设置为 Untrust。

② 目的域：设置域间策略规则的目的区域，在此设置为 DMZ。

③ 规则 ID：给该域间策略规则设置一个 ID 号，在此设置为最小 ID 号 0。

④ 源 IP 地址：设置域间策略规则的源 IP 地址，可以选择新建一个 IP 地址资源或者直接引用已经存在的 IP 地址资源。其中新建 IP 地址是通过给出 IP 地址和通配符掩码来指定一个地址段；而直接引用的 IP 地址资源中默认只存在 any_address，即所有地址，如果需要指定某一个或几个地址段，可以在导航栏中选择“资源管理＞地址＞IP 地址”，在相应的界面下配置主机地址、范围地址或者子网地址，并且可以在“资源管理＞地址＞地址组”界面下创建一个 IP 地址组，将多个已创建的地址段加入到一个地址组中。在本例中源 IP 地址直接选择 any_address，即允许所有 Untrust 域中的主机。

⑤ 目的 IP 地址：设置域间策略规则的目的 IP 地址，在此设置为 10.1.2.10/0.0.0.0，即 FTP Server 的 IP 地址。

⑥ 服务名称：设置域间策略规则中的服务类型，即该规则针对哪一种服务进行安全访问控制。防火墙本身对一些服务进行了预定义，可以在下拉框中选择需要的服务类型。如果需要选择防火墙没有预定义的服务，可以在“资源管理＞服务＞自定义服务”界面下单击“新建”按钮，通过指定相应的端口号来新建服务，并且可以在“资源管理＞服务＞服务组”界面下创建一个服务组，将多个已创建的服务加入到一个服务组中。在本例中，因为要允许 Untrust 域中的主机访问 FTP 服务，因此单击服务名称右侧的“多选”按钮，选择其中的 ftp、ftp-get 和 ftp-put 3 个服务，如图 5-11 所示。

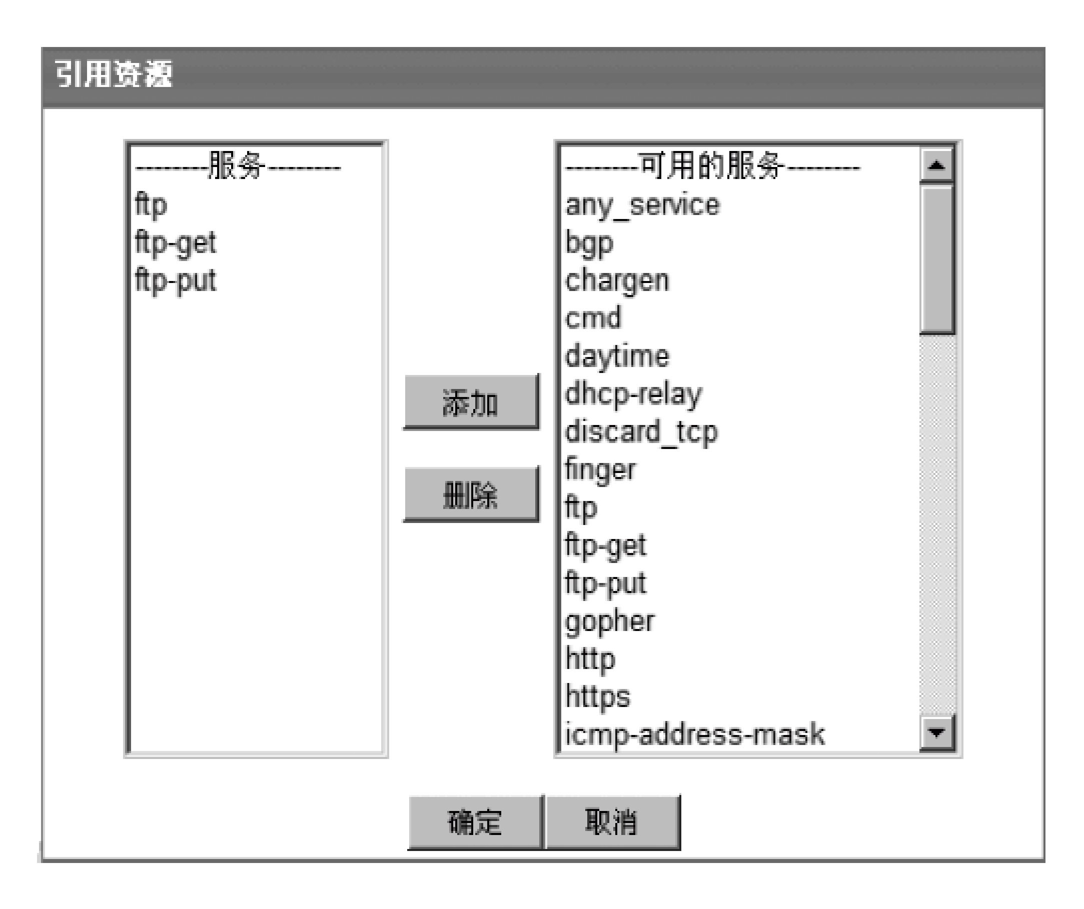


图 5-11　选择多种服务

⑦ 过滤动作：设置对匹配域间策略规则的数据报文进行的操作，在此选择 Permit。

⑧ 时间段：设置域间策略规则生效的时间段。需要首先在“资源管理>时间段”界面下创建时间段，然后才能在这里进行选择。在此不对时间段进行设置，即该域间策略规则一致处于有效状态。

第一条规则配置完成后，继续配置第二条规则，允许 Untrust 域中的主机访问 DMZ 域中的 HTTP Server。两条规则都配置完成后，在域间策略管理界面的显示如图 5-12 所示。



源域	目的域	规则ID	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
Untrust	DMZ	0	any_address	10.1.2.10/0.0.0.0	ftp, ftp-get, ftp-put		Permit		禁止	未开启			
Untrust	DMZ	1	any_address	10.1.2.20/0.0.0.0	http		Permit		禁止	未开启			

图 5-12　域间策略配置情况

在 PC_2 上使用 IE 测试，应该可以访问 FTP Server 上的 FTP 服务和 HTTP Server 上的 HTTP 服务。在“防火墙>安全策略>策略匹配统计”界面下可以看到数据报文匹配情况，如图 5-13 所示。



源域	目的域	允许包数	拒绝包数	开始时间	结束时间	操作
Untrust	DMZ	20	5	2012/01/10 16:35:16	2012/01/10 17:34:50	[清零]

图 5-13　策略匹配统计

(2) NAT 配置

在实际的网络应用中，出于节约 IP 地址和保护内部网络的原因，有些时候还需要配置网络地址转换。在 5.2 节配置的基础上配置 NAT，要求内部网络通过 Easy IP 的方式访问外部网络，而 FTP Server 和 HTTP Server 则通过 NAT Server 将 FTP 服务和 HTTP 服务映射到防火墙接口 GigabitEthernet0/3 的对应端口上。

① Easy IP 配置。首先，在防火墙上创建一个 ACL 来匹配需要进行 Easy IP 转换的内部本地地址，在导航栏中选择“防火墙>ACL”，进入 ACL 管理界面，单击“新建”按钮，新建一个基本 ACL，如图 5-14 所示。

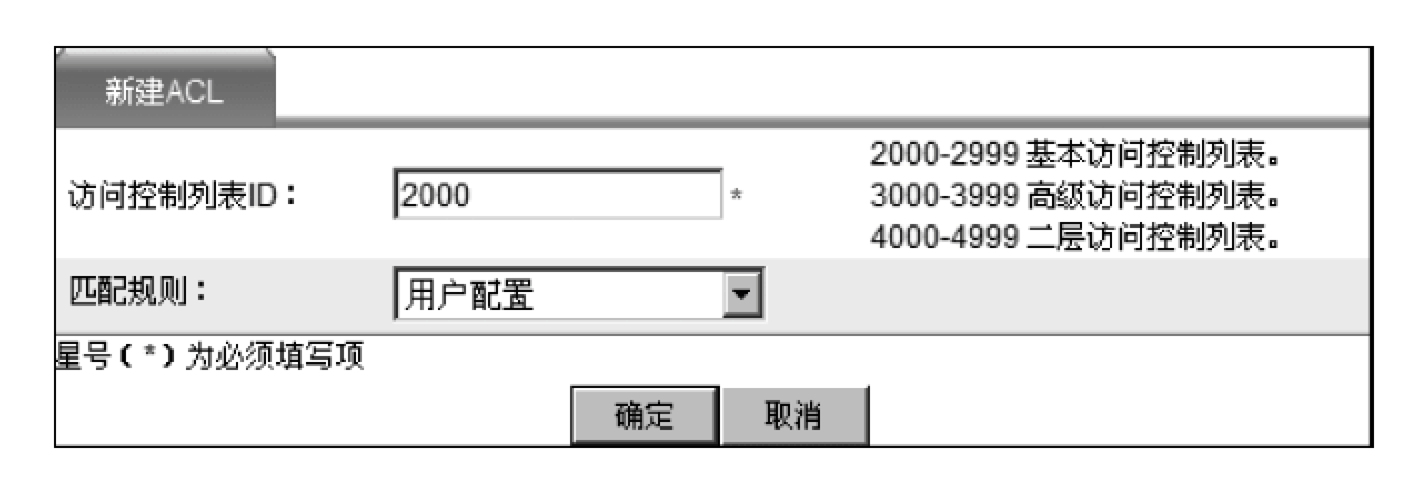


图 5-14　新建 ACL

新建 ACL 后，在 ACL 管理界面单击相应 ACL 右侧“操作”字段下的“编辑 ACL”图标，进入相应 ACL 的编辑界面，在 ACL 编辑界面单击“新建”按钮，新建一条允许源 IP 地址 10.1.1.0/24 的 ACL 规则，如图 5-15～图 5-17 所示。

访问控制列表ID	类型	规则数量	匹配顺序	ACL加速管理	操作
2000	基本	0	用户配置	加速	

图 5-15　ACL 管理界面

基本ACL2000

规则ID	操作	描述	时间段	操作

新建　返回

图 5-16　ACL 编辑界面

ACL=2000 新建基本规则

☐ 规则ID：　（0-65534。如果不输入规则ID，系统将会自动指定一个。）
操作：允许　　时间段：无限制
☐ 分片报文　　☐ 记录日志
☑ 源IP地址：10.1.1.0　　源地址通配符：0.0.0.255
VPN实例：无
确定　取消

图 5-17　新建 ACL 规则

ACL 配置完成后，在导航栏中选择“防火墙>NAT>动态地址转换”，进入到动态地址转换管理界面，如图 5-18 所示。

单击地址转换关联下的“新建”按钮，新建一个动态地址转换，在防火墙接口 GigabitEthernet0/3 上应用地址转换，使 ACL 2000 匹配的内部本地地址通过 Easy IP 的方式过载到防火墙的 GigabitEthernet0/3 接口上，如图 5-19 所示。

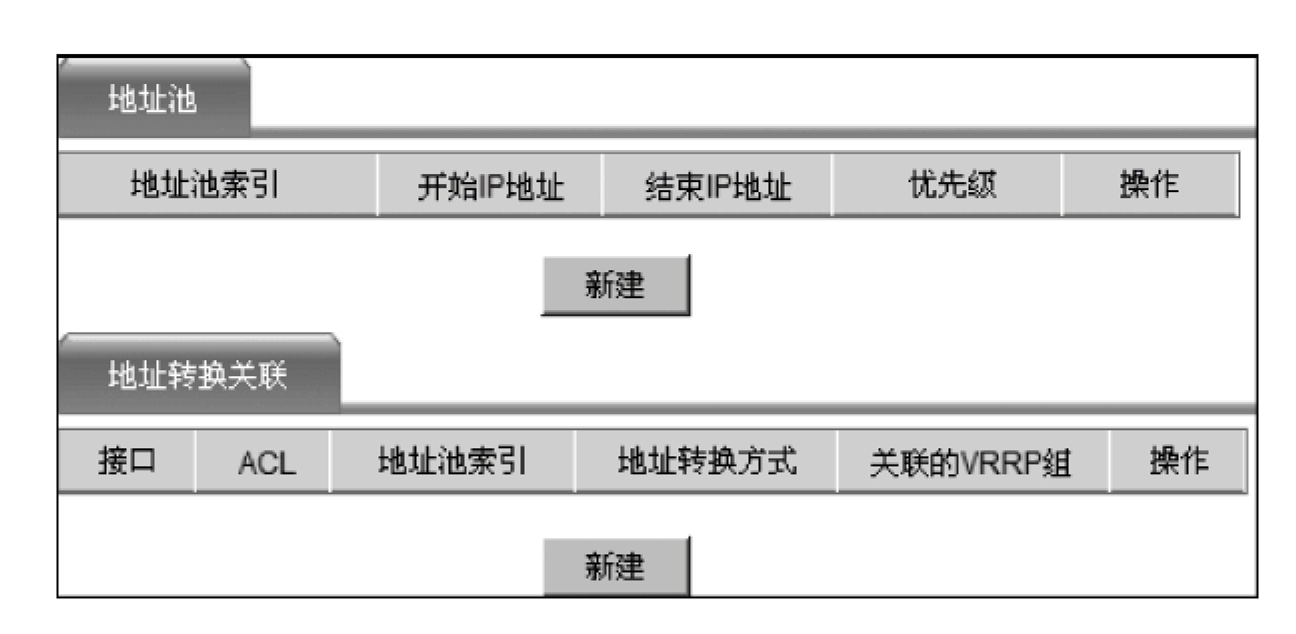


图 5-18　动态地址转换管理界面

新建动态地址转换
接口：GigabitEthernet0/3
ACL：2000 *（2000－3999）
地址转换方式：Easy IP
地址池索引：（0－31）
使能VRRP关联　关联的VRRP组：（1－255）
星号（*）为必须填写项
确定　取消

图 5-19　新建动态地址转换

② NAT Server 配置。在导航栏中选择“防火墙>NAT>内部服务器”，进入到内部服务器转换管理界面，如图 5-20 所示。

内部服务器转换

接口	VPN实例	外部IP地址	外部端口	内部IP地址	内部端口	协议类型	关联的VRRP组	操作

新建

DNS-MAP

域名	外部IP地址	外部端口	协议类型	操作

新建

图 5-20　内部服务器转换管理界面

单击内部服务器转换下的“新建”按钮，新建一个 NAT Server，将 FTP Server 的“IP 地址 10.1.2.10＋端口号 21”映射到防火墙接口 GigabitEthernet0/3 的“IP 地址 202.207.120.1＋端口号 21”上，如图 5-21 所示。

需要注意的是，防火墙与路由器相同，都不能、也不需要对 FTP 的数据端口 20 进行 NAT Server 的配置，具体可参考 3.13.2 小节 NAT Server 与 Easy IP 配置及验证实训。

继续创建 NAT Server，将 HTTP Server 的“IP 地址 10.1.2.20＋端口号 80”映射到防火墙接口 GigabitEthernet0/3 的“IP 地址 202.207.120.1＋端口号 80”上。配置完成后，在内部服务器转换管理界面下可以看到两条 NAT Server 转换配置，如图 5-22 所示。



图 5-21 FTP Server 的 NAT Server 配置

接口	VPN实例	外部IP地址	外部端口	内部IP地址	内部端口	协议类型	关联的VRRP组	操作
GigabitEthernet0/3		202.207.120.1	21	10.1.2.10	ftp	6(TCP)		
GigabitEthernet0/3		202.207.120.1	80	10.1.2.20	www	6(TCP)		

图 5-22 NAT Server 记录

Easy IP 和 NAT Server 都配置完成后，在内网主机 PC_1 上 ping 外网主机 PC_2，同时在 PC_2 上使用 Wireshark 捕获数据报文，从捕获的 ICMP 报文中可以看到与 PC_2 通信的 IP 地址为 202.207.120.1，即防火墙接口 GigabitEthernet0/3 的 IP 地址。在防火墙导航栏中选择"防火墙＞会话管理＞会话列表"，从会话列表中也可以看到 PC_1 的 IP 地址 10.1.1.2 到防火墙接口 GigabitEthernet0/3 的 IP 地址 202.207.120.1 的 Easy IP 转换，如图 5-23 所示。

□	发起方源IP地址	发起方目的IP地址	发起方 VPN / VLAN / INLINE	响应方源IP地址	响应方目的IP地址	响应方 VPN / VLAN / INLINE	协议	会话状态	存活时间(秒)	操作
□	192.168.0.2:4621	192.168.0.1:80	---	192.168.0.1:80	192.168.0.2:4621	---	TCP	TCP-EST	3599	
□	192.168.0.2:4618	192.168.0.1:80	---	192.168.0.1:80	192.168.0.2:4618	---	TCP	FIN-CLOSED	24	
□	10.1.1.2:2048	202.207.120.2:512	---	202.207.120.2:0	202.207.120.1:1027	---	ICMP	ICMP-CLOSED	28	

图 5-23 Easy IP 转换会话

从 PC_2 上使用 IE 通过防火墙接口 GigabitEthernet0/3 的 IP 地址 202.207.120.1 分别访问 FTP 服务和 HTTP 服务，可以访问。从防火墙的会话列表中可以看到 FTP Server 的"IP 地址 10.1.2.10＋端口号 21"到防火墙接口 GigabitEthernet0/3 的"IP 地址202.207.120.1＋端口号 21"的转换和 HTTP Server 的"IP 地址 10.1.2.20＋端口号 80"到防火墙接口 GigabitEthernet0/3 的"IP 地址 202.207.120.1＋端口号 80"的转换，如图 5-24 所示。

3. 混合模式的配置

混合模式是指防火墙同时工作在透明模式和路由模式下，即防火墙的有些接口工作在

□	发起方源IP地址	发起方目的IP地址	发起方 VPN / VLAN / INLINE	响应方源IP地址	响应方目的IP地址	响应方 VPN / VLAN / INLINE	协议	会话状态	存活时间(秒)	操作
□	202.207.120.2:1427	202.207.120.1:80	---	10.1.2.20:80	202.207.120.2:1427	---	TCP	FIN-CLOSED	28	
□	10.1.2.10:137	10.1.2.255:137	---	10.1.2.255:137	10.1.2.10:137	---	UDP	UDP-OPEN	25	
□	202.207.120.2:1430	202.207.120.1:21	---	10.1.2.10:21	202.207.120.2:1430	---	TCP	TCP-EST	3592	
□	202.207.120.2:60412	202.99.160.68:53	---	0.0.0.0:0	0.0.0.0:0	---	UDP	UDP-OPEN	0	
□	192.168.0.2:4798	192.168.0.1:80	---	192.168.0.1:80	192.168.0.2:4798	---	TCP	FIN-CLOSED	10	
□	192.168.0.2:4804	192.168.0.1:80	---	192.168.0.1:80	192.168.0.2:4804	---	TCP	TCP-EST	3600	

图 5-24　NAT Server 转换会话

数据链路层，而有些接口工作在网络层。混合模式可以满足企业网络多样化的部署要求。

假设存在如图 5-25 所示的网络，其中 GigabitEthernet0/1 连接的网络属于 Trust 域，GigabitEthernet0/2 连接的网络属于 DMZ 域，GigabitEthernet0/3 连接的网络属于 Untrust 域。Trust 域和 DMZ 域处于同一个网段 10.1.1.0/24，GigabitEthernet0/1 和 GigabitEthernet0/2 为桥模式，都属于 VLAN 100，三层虚接口 vlan-interface 100 的 IP 地址为 10.1.1.1/24；GigabitEthernet0/3 为路由模式，IP 地址为 202.207.120.1/24。

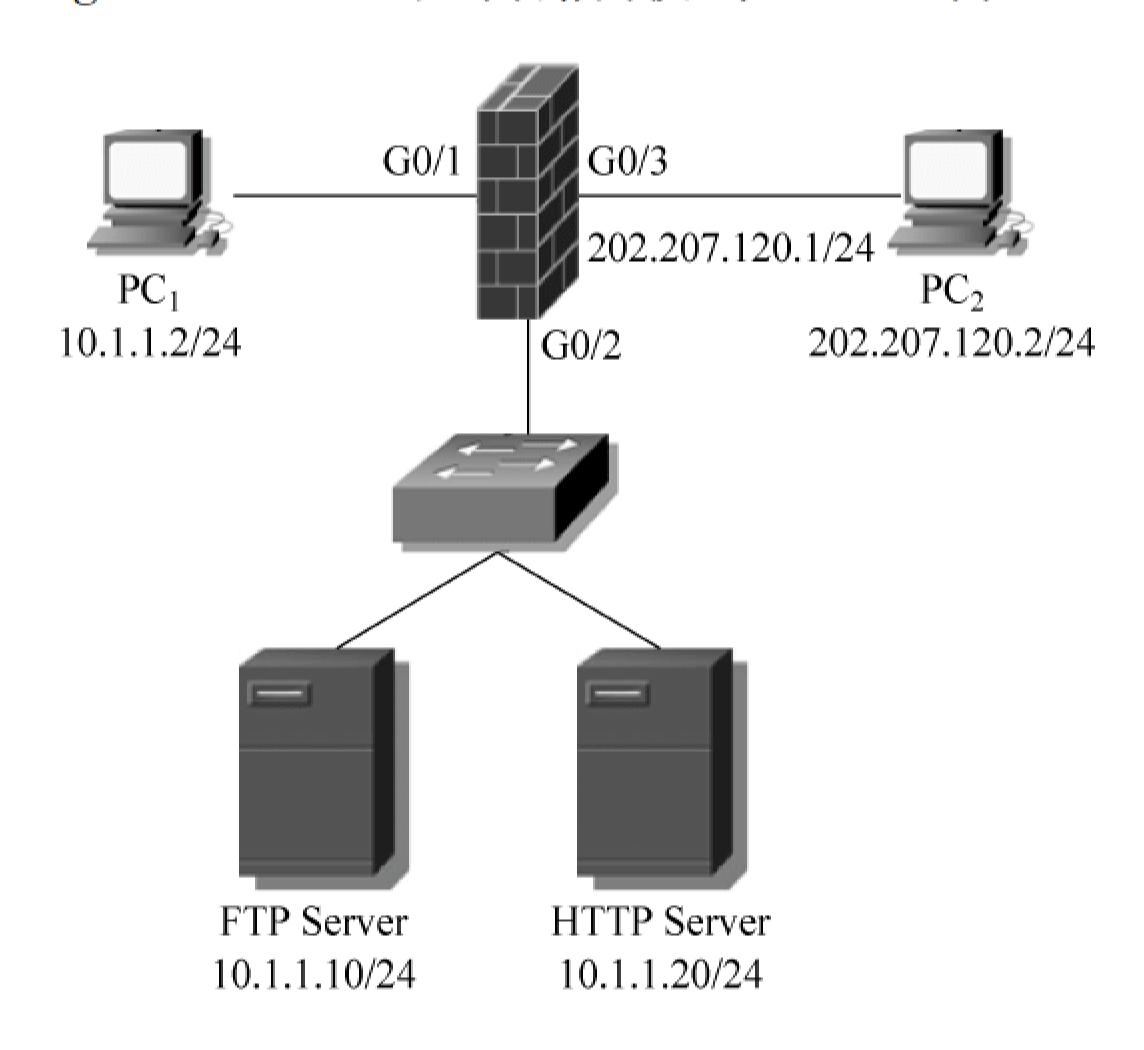


图 5-25　混合模式配置

首先在防火墙上创建 VLAN 100，将接口 GigabitEthernet0/1 和 GigabitEthernet0/2 设置为桥模式并划分到 VLAN 100 中，为三层虚接口 vlan-interface 100 和接口 GigabitEthernet0/3 分别配置相应的 IP 地址。

将接口 GigabitEthernet0/1 加入到 Trust 域，将接口 GigabitEthernet0/2 加入到 DMZ 域，将接口 GigabitEthernet0/3 加入到 Untrust 域，将三层虚接口 vlan-interface 100 加入到 Trust 域中。

注意：在 PC_1 与 FTP Server/HTTP Server 之间互相访问时，数据流量的出入安全域均由物理接口所在的安全域决定，与三层虚接口 vlan-interface 100 所在的安全域无关。因为 PC_1 和 FTP Server/HTTP Server 处于同一个网段中，接口 GigabitEthernet0/1 和 GigabitEthernet0/2 之间工作在透明模式，互相访问不需要通过网关(即三层虚接口 vlan-interface 100)地址。这一点可以通过将三层虚接口 vlan-interface 100 加入到 DMZ

域或 Untrust 域中,然后在 PC_1 和 FTP Server/HTTP Server 之间互访来进行测试。通过测试会发现无论将三层虚接口 vlan-interface 100 加入到哪一个安全域中,对测试结果都没有任何影响,均为 PC_1 可以访问 FTP Server/HTTP Server,但 FTP Server/HTTP Server 不能访问 PC_1。

在 PC_1 和 FTP Server/HTTP Server 与 PC_2 互相访问时,PC_2 的出入安全域由物理接口 GigabitEthernet0/3 所在的安全域决定,但 PC_1 和 FTP Server/HTTP Server 的出入安全域由三层虚接口 vlan-interface 100 所在的安全域决定。这是因为 PC_1 和 FTP Server/HTTP Server 与 PC_2 之间的互相访问属于跨网段的访问,因此对于 PC_1 和 FTP Server/HTTP Server 而言,其安全域将由网关所在的安全域决定。这一点可以通过以下几个测试来进行验证。

(1) 将三层虚接口 vlan-interface 100 加入到 Untrust 域,通过测试会发现 PC_1 与 PC_2 之间、FTP Server/HTTP Server 与 PC_2 之间均可以互访,这是因为同属一个安全区域的网络之间可以互相访问。但要注意,FTP Server/HTTP Server 不能访问 PC_1。

(2) 将三层虚接口 vlan-interface 100 加入到 Trust 域,如果需要允许 PC_2 访问 FTP Server/HTTP Server,则需要配置 Untrust 域到 Trust 域之间的策略,而不是配置 Untrust 域到 DMZ 域之间的策略。

(3) 将三层虚接口 vlan-interface 100 加入到 DMZ 域,如果需要允许 PC_2 访问 PC_1,则需要配置 Untrust 域到 DMZ 域之间的策略,而不是配置 Untrust 域到 Trust 域之间的策略。

注意:一定要将三层虚接口 vlan-interface 100 加入到一个安全域中,否则从防火墙本身发起的在 vlan-interface 100 网段中的广播和多播报文(如路由协议报文等)将无法发出。在这里建议将三层虚接口 vlan-interface 100 加入到 Trust 域中,以保障处于不同安全区域但在同一逻辑网段中的设备均能够接收到相应的广播和多播报文。

域间策略和 NAT 的配置与 5.2.2 小节类似,在此不再赘述。

5.3.2 Cisco 设备配置

在 Cisco 的 PIX 系列防火墙上,安全级别针对接口进行设置,防火墙的基本配置涉及的命令如下。

(1) 配置接口名称

```
Firewall (config-if) # nameif {inside|outside|dmz|name}
```

Cisco PIX 防火墙的接口必须首先被命名,然后其 IP 功能才能被启用。可以将一个接口命名为 inside、outside、dmz 或任意一个字符串,如果将接口命名为 inside,则接口的安全级别自动被设置为 100;如果将接口命名为 outside、dmz 或其他字符串时,则接口的安全级别自动被设置为 0。

(2) 配置接口的安全级别

```
Firewall (config-if) # security-level level
```

可以根据需要修改系统自动设置的安全级别,例如,将 DMZ 接口的安全级别设置为 50。参数 *level* 的取值范围为 1～100。

(3) 配置静态路由

```
Firewall (config)# route interface destination-address destination-netmask next-hop-address
```

与路由器上配置静态路由的命令不同,在 Cisco PIX 防火墙上配置静态路由,需要使用 interface 参数指定防火墙的送出接口。

(4) 地址转换的配置

① 静态 NAT 的配置。

```
Firewall (config)# static (interface1, interface2) global-ip local-ip
```

其中,参数 *interface*1 和 *interface*2 分别是指地址转换的内部接口和外部接口。

② 动态 NAT 和 NAPT 的配置。

```
Firewall (config)# global (interface) pool-id {startaddress-endaddress|startaddress|interface}
Firewall (config)# nat (interface) pool-id {local-ip netmask|acl-number}
```

global 命令用来定义存放内部全局地址的地址池,该地址池由 pool-id 唯一地标识,如果地址池中定义了一个地址范围,则转换为动态 NAT;如果地址池中只定义了一个地址,则转换为 NAPT;如果地址池定义中直接给出单词 interface,则意味着将是一个 Easy IP 的转换。如果需要将内部本地地址通过 NAPT 转换到多个内部全局地址上,则需要配置多条 global 命令。

在 global 命令中小括号中的参数 *interface* 是指内部全局地址对应的接口,即进行地址转换的外部接口;在 nat 命令中小括号中的参数 *interface* 是指内部本地地址对应的接口,即进行地址转换的内部接口。

③ 端口地址重定向的配置。

```
Firewall (config)# static (interface1, interface2) {tcp|udp} {global-ip|interface} global-port
local-ip local-port
```

在端口地址重定向的配置中,如果给出的全局参数为 *global-ip*,意味着将重定向到该 IP 地址对应的端口上;如果给出的全局参数为单词 interface,则意味着将重定向到 *interface*2 参数对应的端口上。

对应于 H3C 防火墙上域间策略的配置,在 Cisco PIX 防火墙上需要通过配置访问控制列表来实现,其配置方法与路由器上的基本相同,在此不再进行介绍。

5.4 模拟公司总部边界防火墙配置方案

根据 5.1 节的安全配置任务,可参考以下方案配置模拟公司总部防火墙,以保障网络通信安全。

(1) 网络联通性配置。如图 5-26 所示,模拟公司总部防火墙外部接口 outside,使用 IP 地址为 200.100.8.126/30;内部接口 inside,使用 IP 地址为 200.100.8.121/30。防火墙通过一个边界路由器连接到 Internet,该路由器内网接口使用 IP 地址为 200.100.8.125,连接 Internet 接口使用 IP 地址为 200.100.15.197。

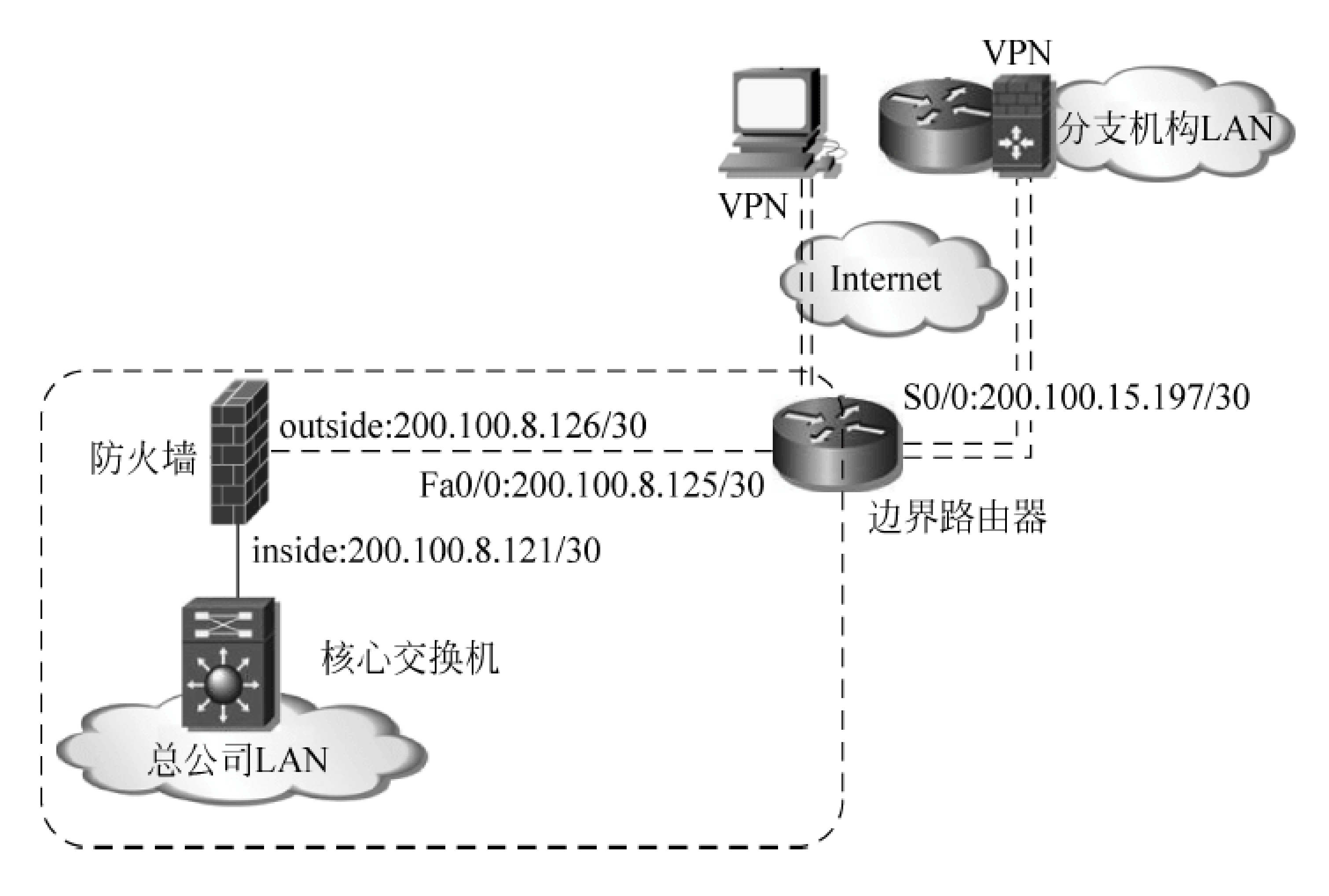


图 5-26　总部边界网络联通性

(2) 配置访问控制,仅允许外部网络访问内部 Web 服务器 200.100.8.27/27,邮件服务器 200.100.8.28/27。

(3) 根据防火墙默认访问规则,从防火墙外网到内网主动 TCP 连接是被默认禁止的,但从内网到外网的连接默认是不受限制的,所以使用防火墙默认模式即可满足要求。

5.5　小结

作为专门的网络安全设备,防火墙为网络提供了比路由器更为强大的安全防护功能。本章首先对防火墙的基本概念,包括安全区域、安全级别以及应用位置等进行了介绍;然后分别对防火墙的3种不同的工作模式进行了介绍;最后简单介绍了 Cisco PIX 防火墙的基本配置。

5.6　习题

1. 按照实现方式的区别,防火墙可以分成哪几种类型?
2. 在 H3C 的防火墙上,共有几个安全区域?其安全级别分别是多少?
3. 请简要描述 H3C 防火墙上的域间策略。
4. 防火墙有哪几种不同的工作模式?分别适用于什么场合?
5. 什么是统一威胁管理设备?

5.7　实训

5.7.1　防火墙路由模式配置实训

实验学时:2学时。

每组实验学生人数:3~4人。

1. 实验目的

(1) 掌握防火墙路由模式的配置方法和域间策略的配置方法。

(2) 理解防火墙的域间安全访问控制的实现。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：4 台

(2) H3C SecPath U200-CA：1 台

(3) 二层交换机：2 台

(4) UTP 电缆：7 条

(5) Console 电缆：1 条

保持防火墙和交换机均为出厂配置。

3. 实验内容

(1) 配置防火墙接口。

(2) 部署安全区域。

(3) 配置域间策略。

(4) 配置网络地址转换。

4. 实验指导

(1) 按照图 5-27 所示的网络拓扑结构搭建网络，完成网络连接。

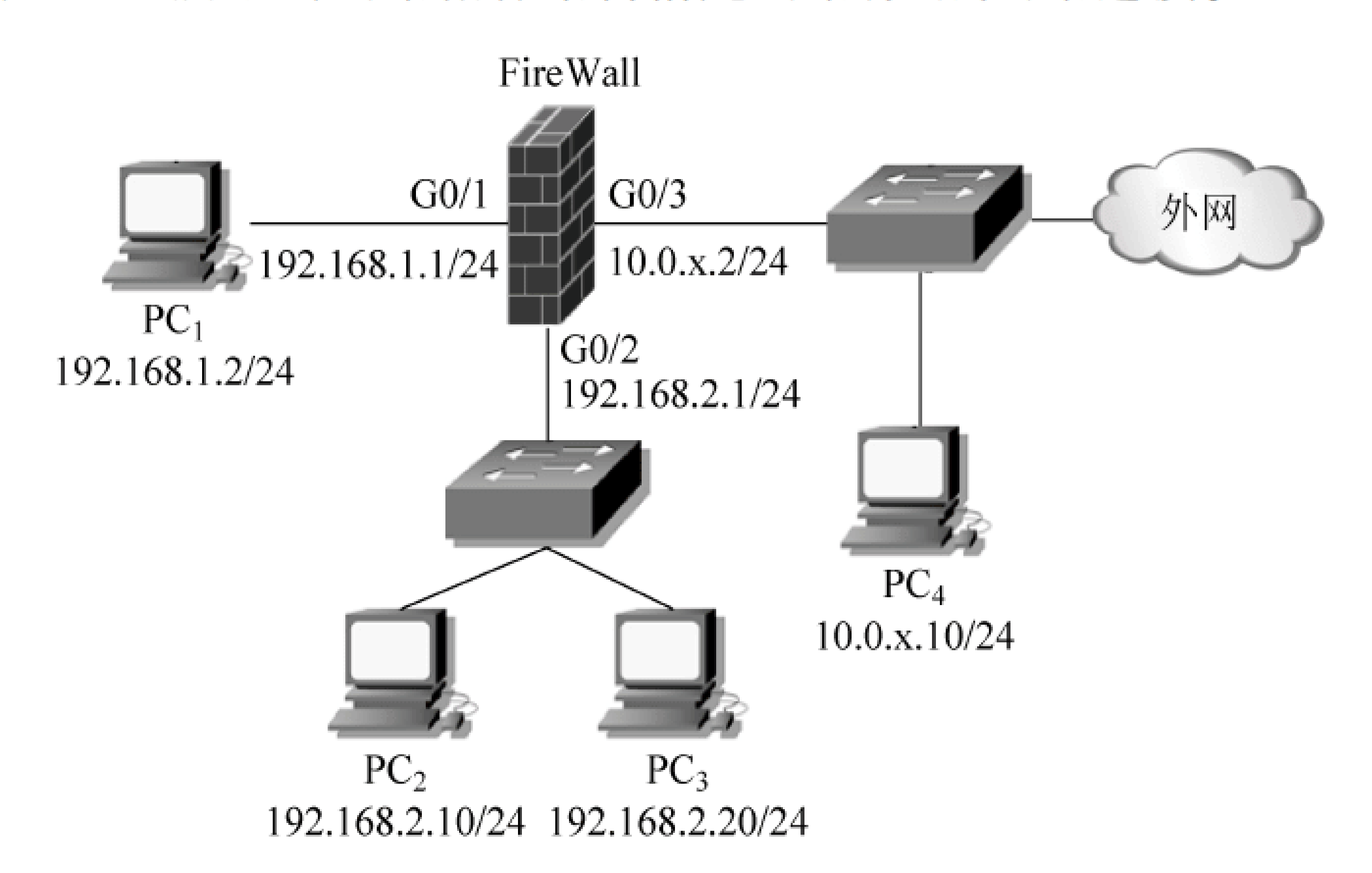


图 5-27　防火墙路由模式配置实训

(2) 按照图 5-27 所示的防火墙的接口和 4 台 PC 配置 IP 地址，注意 PC_4 的默认网关需要配置为 10.0.x.2，两台交换机均保持空配置。

(3) 在 PC_2 和 PC_3 上启动 XAMPP 软件，在 PC_2 上开启 FileZilla 服务，即开启 FTP 服务；在 PC_3 上开启 Apache 服务，即开启 HTTP 服务。

(4) 在防火墙上，将接口 GigabitEthernet0/1、GigabitEthernet0/2 和 GigabitEthernet0/3 分别划分到 Trust、DMZ 和 Untrust 域中。

配置完成后，在 4 台 PC 之间使用 ping 命令进行网络联通性测试，PC_1 应该可以访问 PC_2、PC_3 和 PC_4；PC_2 和 PC_3 可以访问 PC_4，但不能访问 PC_1；PC_4 无法访问 PC_1、PC_2 和

PC_3,与防火墙的默认域间策略相符合。

(5) 配置域间策略,要求外部网络主机可以访问 PC_2 上的 FTP 服务和 PC_3 上的 HTTP 服务。具体配置方法参考 5.2.2 小节的域间策略配置部分,配置完成后,在防火墙的域间策略管理界面上查看域间策略,如图 5-28 所示。

□	源域	目的域	规则ID	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
□	Untrust	DMZ	0	any_address	192.168.2.10/0.0.0.0	ftp, ftp-get, ftp-put		Permit		禁止	未开启			
□	Untrust	DMZ	1	any_address	192.168.2.20/0.0.0.0	http		Permit		禁止	未开启			

图 5-28　域间策略配置

在 PC_4 上使用 IE 进行测试,应该可以访问 PC_2 上的 FTP 服务和 PC_3 上的 HTTP 服务。

(6) 在防火墙上配置去往外部网络的默认路由。参考命令如下:

```
[FireWall]ip route-static 0.0.0.0 0 10.0.x.1
```

(7) 配置网络地址转换,要求在命令行下进行配置,使内部网络通过 Easy IP 的方式访问外部网络,而 PC_2 和 PC_3 则通过 NAT Server 将 FTP 服务和 HTTP 服务映射到防火墙接口 GigabitEthernet0/3 的对应端口上。

参考命令如下:

```
[FireWall]acl number 2000
[FireWall-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[FireWall-acl-basic-2000]quit
[FireWall]interface GigabitEthernet 0/3
[FireWall-GigabitEthernet0/3]nat outbound 2000
[FireWall-GigabitEthernet0/3]nat server protocol tcp global 10.0.x.2 21 inside 192.168.2.10 21
[FireWall-GigabitEthernet0/3]nat server protocol tcp global 10.0.x.2 80 inside 192.168.2.20 80
```

配置完成后,在 PC_4 上使用 IE 进行测试,通过防火墙接口 GigabitEthernet0/3 的 IP 地址 10.0.x.2 分别访问 FTP 服务和 HTTP 服务,应该可以访问,从防火墙的会话列表中可以看到相应的 NAT Server 转换。在 PC_1 上可以访问外部网络(如百度网站),从防火墙的会话列表中可以看到相应的 Easy IP 转换。

5. 实验报告

<table>
<tr><td rowspan="4">默认域间策略</td><td></td><td>Trust 域</td><td>DMZ 域</td><td>Untrust 域</td></tr>
<tr><td>Trust 域</td><td></td><td></td><td></td></tr>
<tr><td>DMZ 域</td><td></td><td></td><td></td></tr>
<tr><td>Untrust 域</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">域间策略配置</td><td colspan="2">源 IP 地址</td><td>目的 IP 地址</td><td>服务</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="2">NAT 配置</td><td>Easy IP 配置</td><td colspan="3"></td></tr>
<tr><td>NAT Server 配置</td><td colspan="3"></td></tr>
<tr><td colspan="2">考虑 PC₁ 为什么可以访问外部网络</td><td colspan="3"></td></tr>
</table>

5.7.2　防火墙混合模式配置实训

实验学时：2 学时。

每组实验学生人数：3～4 人。

1. 实验目的

(1) 掌握防火墙混合模式的配置方法。

(2) 理解三层虚接口在安全域中的作用。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：4 台

(2) H3C SecPath U200-CA：1 台

(3) 二层交换机：2 台

(4) UTP 电缆：7 条

(5) Console 电缆：1 条

保持防火墙和交换机均为出厂配置。

3. 实验内容

(1) 配置防火墙接口。

(2) 部署安全区域。

(3) 配置域间策略。

(4) 配置网络地址转换。

4. 实验指导

(1) 按照图 5-29 所示的网络拓扑结构搭建网络，完成网络连接。

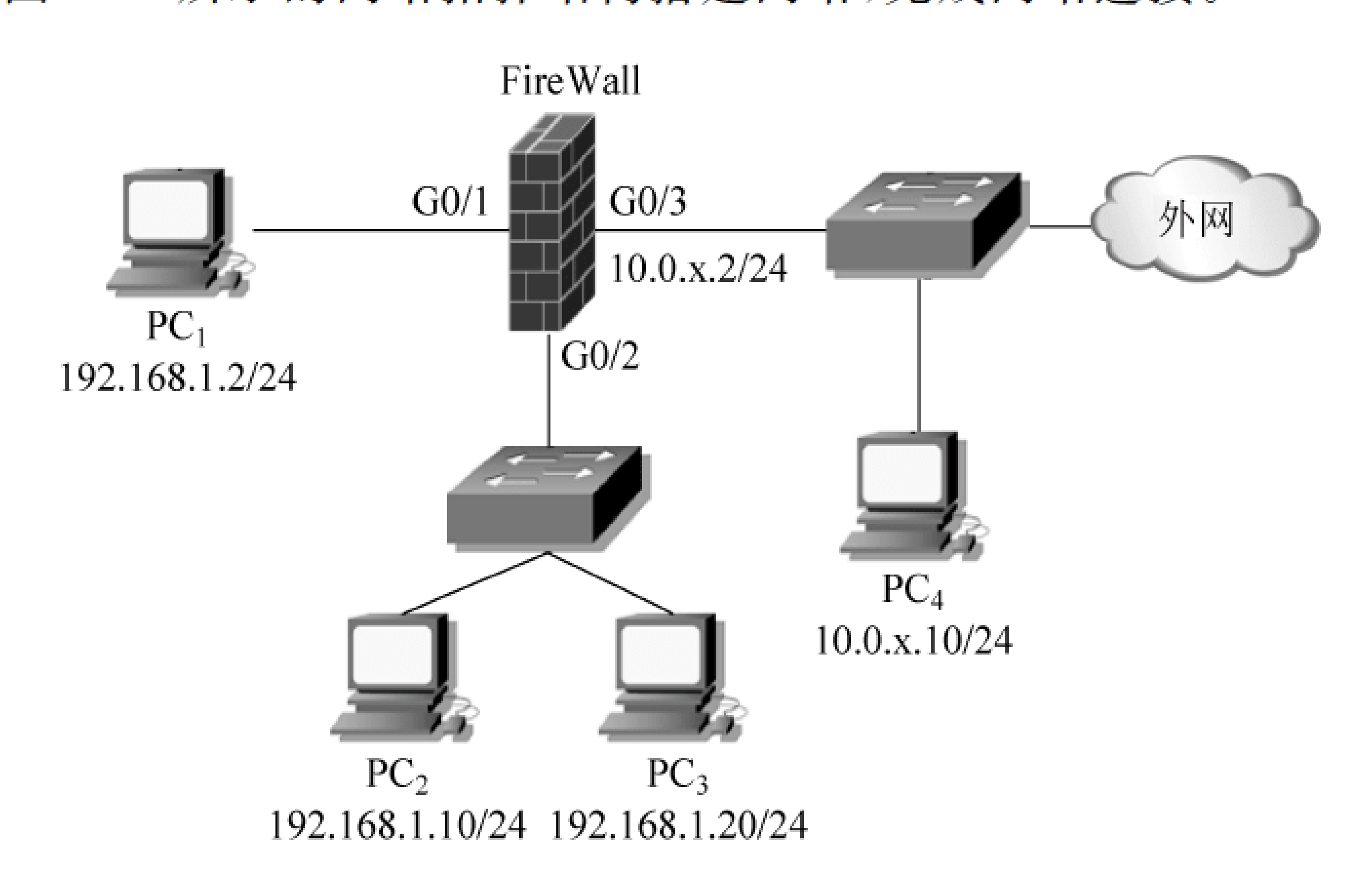


图 5-29　防火墙混合模式配置实训

(2) 按照图 5-29 所示为防火墙的接口 GigabitEthernet0/3 和 4 台 PC 配置 IP 地址，其中注意 PC_4 的默认网关需要配置为 10.0.x.2；在防火墙上创建 VLAN 10，将接口 GigabitEthernet0/1 和 GigabitEthernet0/2 均设置为桥模式，并划分到 VLAN 10 中，为三层虚接口 vlan-interface 10 配置 IP 地址 192.168.1.1/24；两台交换机均保持空配置。

(3) 在 PC_2 和 PC_3 上启动 XAMPP 软件，在 PC_2 上开启 FileZilla 服务，即开启 FTP

服务;在 PC_3 上开启 Apache 服务,即开启 HTTP 服务。

(4) 在防火墙上,将接口 GigabitEthernet0/1、GigabitEthernet0/2 和 GigabitEthernet 0/3 分别划分到 Trust、DMZ 和 Untrust 域中;将三层虚接口 vlan-interface 10 加入到 Trust 域中。

配置完成后,在 4 台 PC 之间使用 ping 命令进行网络联通性测试,PC_1 可以访问 PC_2、PC_3 和 PC_4;PC_2 和 PC_3 可以访问 PC_4,但不能访问 PC_1;PC_4 无法访问 PC_1、PC_2 和 PC_3。

(5) 配置域间策略,要求外部网络主机可以访问 PC_2 上的 FTP 服务和 PC_3 上的 HTTP 服务。

在这里有两种配置方案:

① 将三层虚接口 vlan-interface 10 加入到 DMZ 域中,然后设置 Untrust 域到 DMZ 域的策略,如图 5-30 所示。

□	源域	目的域	规则ID	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
□	Untrust	DMZ	0	any_address	192.168.1.10/0.0.0.0	ftp, ftp-get, ftp-put		Permit		禁止	未开启			
□	Untrust	DMZ	1	any_address	192.168.1.20/0.0.0.0	http		Permit		禁止	未开启			

图 5-30 域间策略配置 1

② 三层虚接口 vlan-interface 10 在 Trust 域中保持不变,设置 Untrust 域到 Trust 域的策略,如图 5-31 所示。

□	源域	目的域	规则ID	源IP地址	目的IP地址	服务	时间段	过滤动作	描述	启用选项	日志功能	源MAC地址	目的MAC地址	操作
□	Untrust	Trust	0	any_address	192.168.1.10/0.0.0.0	ftp, ftp-get, ftp-put		Permit		禁止	未开启			
□	Untrust	Trust	1	any_address	192.168.1.20/0.0.0.0	http		Permit		禁止	未开启			

图 5-31 域间策略配置 2

注意:在图 5-31 中设置的域间策略,目的 IP 地址为处于 DMZ 域中的 PC_2 和 PC_3 的 IP 地址,但目的域为 Trust 域,这是因为在外部网络访问 PC_2 和 PC_3 时,出安全域将由三层虚接口 vlan-interface 10 所在的安全域决定。

配置完成后,在 PC_4 上使用 IE 进行测试,应该可以访问 PC_2 上的 FTP 服务和 PC_3 上的 HTTP 服务。

(6) 在防火墙上配置去往外部网络的默认路由。参考命令如下:

```
[FireWall]ip route-static 0.0.0.0 0 10.0.x.1
```

(7) 配置网络地址转换,要求在命令行下进行配置,使内部网络通过 Easy IP 的方式访问外部网络,而 PC_2 和 PC_3 则通过 NAT Server 将 FTP 服务和 HTTP 服务映射到防火墙接口 GigabitEthernet0/3 的对应端口上。

参考命令如下:

```
[FireWall]acl number 2000
[FireWall-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[FireWall-acl-basic-2000]quit
[FireWall]interface GigabitEthernet 0/3
```

```
[FireWall-GigabitEthernet0/3]nat outbound 2000
[FireWall-GigabitEthernet0/3]nat server protocol tcp global 10.0.x.2 21 inside 192.168.1.10 21
[FireWall-GigabitEthernet0/3]nat server protocol tcp global 10.0.x.2 80 inside 192.168.1.20 80
```

配置完成后，在 PC_4 上使用 IE 进行测试，通过防火墙接口 GigabitEthernet0/3 的 IP 地址 10.0.x.2 分别访问 FTP 服务和 HTTP 服务，应该可以访问，从防火墙的会话列表中可以看到相应的 NAT Server 转换。在 PC_1、PC_2 和 PC_3 上应该都可以访问外部网络(如百度网站)，从防火墙的会话列表中可以看到相应的 Easy IP 转换。

5. 实验报告

vlan-interface 10 在 DMZ 域中时域间策略配置	源 IP 地址	目的 IP 地址	服务
vlan-interface 10 在 Trust 域中时域间策略配置	源 IP 地址	目的 IP 地址	服务
出入安全域		入安全域	出安全域
	PC_1 访问 PC_2/PC_3		
	PC_1 访问 PC_4		
	PC_2/PC_3 访问 PC_4		
	PC_4 访问 PC_2/PC_3		
	考虑在什么时候数据流量的出入安全域由三层虚接口所在的安全域决定		
NAT 配置	Easy IP 配置		
	NAT Server 配置		

第 6 章

局域网安全

本章任务：根据工程任务安全需求分析，解决局域网中的安全配置问题。

必备知识：（1）AAA 技术。

（2）IEEE 802.1x 技术。

（3）端口安全技术。

（4）端口绑定技术。

（5）DHCP Snooping 技术。

学习目标：完成模拟公司总部局域网的网络安全配置，防御局域网内常见的安全威胁。

6.1 模拟网络局域网安全任务分析

模拟公司总部局域网拓扑如图 6-1 所示。

用户数据流量由分布在各楼层的二层交换机接入网络，又经分布在各楼宇的三层交换机汇聚，最终进入位于网络中心的核心交换机高速转发。在这样的交换网络中，可能会存在以下安全问题从而影响网络的正常运行。

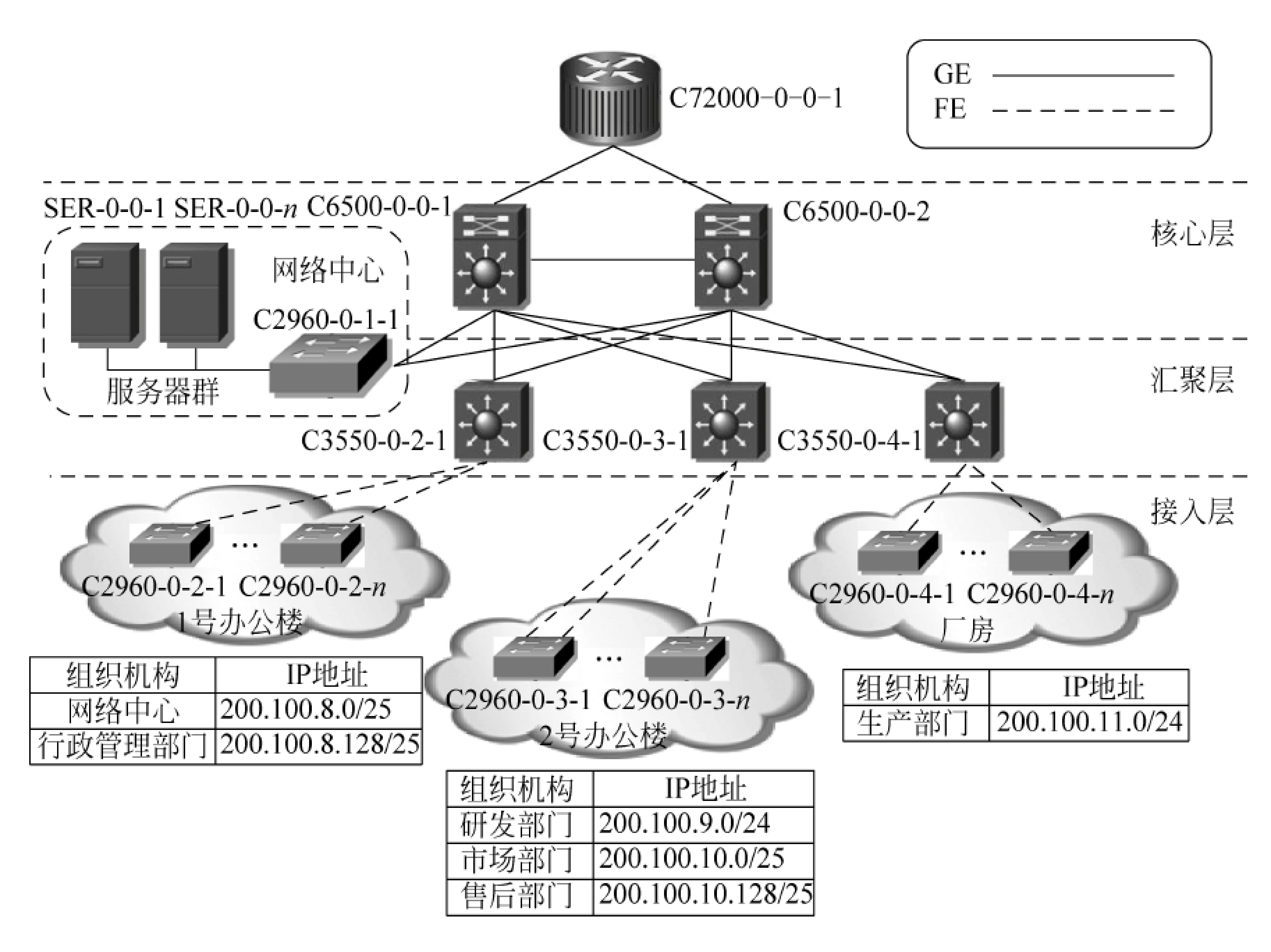
（1）网络中存在大量的网络设备，分散的设备管理一方面增加了网络管理员管理的复杂度；另一方面在网络设备受到攻击后，本地认证方式难以查询攻击时间、攻击事件和攻击者的信息，从而难以进一步进行网络安全防护。

（2）由于办公网络的开放性，很难控制用户私自向网络中接入网络设备和主机，也很难防止恶意用户未经授权接入办公网络。

（3）由于从 Internet 上可以轻易获得各类局域网攻击工具，因此模拟公司总部网络有被恶意用户进行诸如 MAC 地址泛洪、MAC 地址欺骗、ARP 欺骗、DHCP 欺骗攻击的安全风险。而一些网络病毒，例如，ARP 病毒则更有可能让公司计算机在毫不知情下发动 ARP 攻击。

要解决以上网络安全问题，可以在模拟公司总部局域网中实施以下局域网安全配置方案，以保障网络的安全。

（1）使用 AAA 技术对网络中网络设备的认证、授权和计费进行集中管理，通过查询



组织机构	IP地址
网络中心	200.100.8.0/25
行政管理部门	200.100.8.128/25

组织机构	IP地址
研发部门	200.100.9.0/24
市场部门	200.100.10.0/25
售后部门	200.100.10.128/25

组织机构	IP地址
生产部门	200.100.11.0/24

图 6-1　模拟公司总部局域网拓扑图

RADIUS 服务器上的计费信息，随时监控网络设备的登录情况，及时发现尝试性的非法登录试探并进行相关处理。

(2) 使用 IEEE 802.1x 技术对所有接入网络的终端用户进行身份的认证和授权，以防范非法用户访问和合法用户的越权访问。

(3) 使用端口安全和端口绑定技术对合法的 IP 地址和 MAC 地址与端口进行绑定，以防范诸如 MAC 地址泛洪、MAC 地址欺骗、ARP 欺骗等网络攻击。

(4) 使用 DHCP Snooping 技术防范恶意用户假冒 DHCP 服务器或 DHCP 客户端对网络中的 DHCP 服务进行 DoS 攻击。

6.2　AAA 技术

AAA(Authentication、Authorization and Accounting，认证、授权和计费)是一个综合的安全架构，它提供了一个对认证、授权和计费这 3 种功能进行统一配置管理的安全框架。其中认证功能用来对访问网络的用户身份进行认证，判断访问者是否为合法用户；授权功能为认证通过的不同用户赋予不同的权限，限制用户可以访问的资源和使用的服务；计费功能用来记录用户的操作和使用的网络资源，包括使用的服务类型、起始时间和数据流量等，在计费的同时对网络安全情况进行监控。AAA 通常采用 C/S 结构，其中客户端运行于被管理的资源一侧，即网络接入服务器(Network Access Server，NAS)上，服务器则集中管理用户信息。

AAA 支持本地和远端进行认证、授权和计费三种方式。

本地认证、授权和计费将用户信息包括本地用户的用户名、密码以及各种属性配置在网络设备(即NAS)上,相当于将NAS和服务器集成在同一个设备上。本地认证、授权和计费相对而言速度快,运营成本较低,但由于用户信息分散在各个网络设备上,在网络规模较大时会增加管理成本。本地认证、授权和计费的配置相对比较简单,具体配置请参考《计算机网络集成技术》(田庚林、张少芳编著,清华大学出版社出版)一书中的第6章网络设备管理与维护。

远端认证、授权和计费需要有专门的服务器来集中管理用户信息,在NAS和服务器之间通过专门的协议进行认证、授权和计费。常用的AAA协议有远程认证拨入用户服务(Remote Authentication Dial-In User Service,RADIUS)协议和终端访问控制器访问控制系统(Terminal Access Controller Access Control System,TACACS+)协议。其中RADIUS协议在传输层基于UDP协议实现,认证和授权绑定在一起;而TACACS+协议在传输层基于TCP协议实现,并且将认证和授权分离,因此TACACS+协议具有更高的安全性,但相对配置和管理也比较复杂。目前AAA最常使用的是RADIUS协议,本节只对RADIUS协议进行介绍。

6.2.1 RADIUS基础

RADIUS协议是一种分布式、C/S结构的信息交互协议,能保护网络不受未授权访问干扰,常被应用在既要求较高的安全性、又要求允许远程用户访问的网络环境中。RADIUS协议最初只是针对拨号用户进行认证、授权和计费,随着用户接入方式的多样化,RADIUS协议被逐渐应用于多种用户接入方式中,如以太网接入、管理用户登录等。它通过认证和授权来提供接入服务,通过计费来收集、记录用户对网络资源的使用情况。

RADIUS协议在传输层基于UDP协议实现,其中认证和授权使用端口号1812,计费端口号为1813。

1. RADIUS认证、授权和计费流程

RADIUS客户端和RADIUS服务器之间通过共享密钥来验证对方身份的合法性并对用户密码进行加密,以增强安全性。RADIUS的具体认证、授权和计费流程如图6-2所示。

(1) 用户发起连接请求,输入用户名和密码。

(2) RADIUS客户端根据获取的用户名和密码,向RADIUS服务器发送认证请求(Access-Request)包,其中包中的用户密码为被共享密钥加密后的密文。

(3) RADIUS服务器将接收到的用户名和密码与自己保存的数据库信息进行对比,如果数据库中存在相应的用户名和密码,则认证成功,RADIUS服务器向RADIUS客户端发送包含用户授权信息的认证接受(Access-Accept)包;如果认证失败,则返回认证拒绝(Access-Reject)包。

(4) RADIUS客户端根据接收到的认证结果接入/挂断用户。如果允许用户接入,则RADIUS客户端向RADIUS服务器发送计费开始请求(Accounting-Request)包。

(5) RADIUS服务器返回计费开始响应(Accounting-Response)包,并开始计费。

(6) RADIUS客户端为用户提供相应的服务。

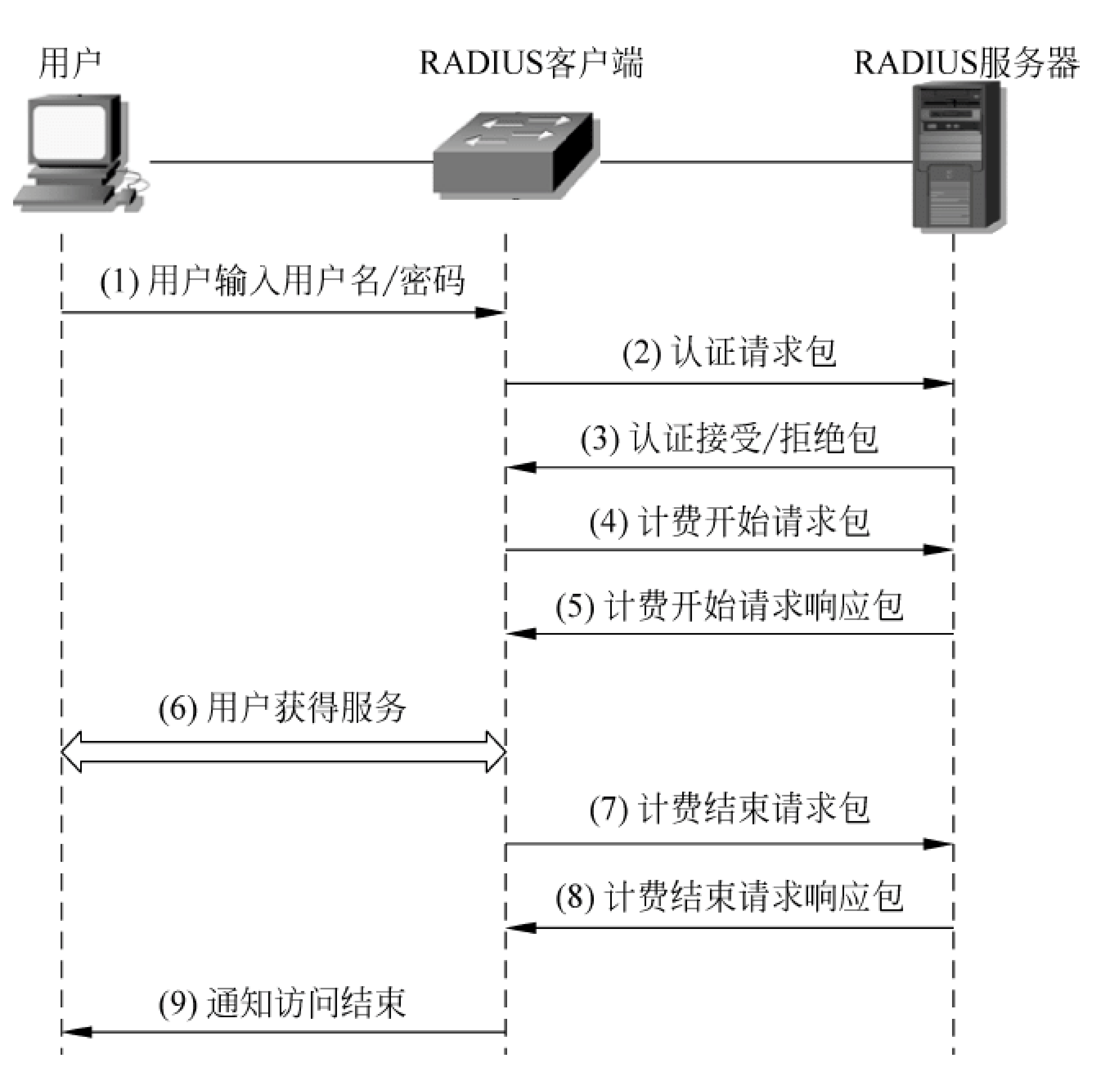


图 6-2　RADIUS 认证、授权和计费流程

(7) 用户请求断开连接，RADIUS 客户端向 RADIUS 服务器发送计费结束请求(Accounting-Request)包。

(8) RADIUS 服务器返回计费结束响应(Accounting-Response)包，并停止计费。

(9) 用户访问资源结束。

其中，计费开始请求包和计费结束请求包均为 Accounting-Request，其区别在于 Acct-Status-Type 属性的取值，计费开始请求包中 Acct-Status-Type 的取值为 Start，而计费结束请求包中 Acct-Status-Type 的取值为 Stop。计费开始响应包和计费结束响应包则为相应请求包的响应。

2. RADIUS 协议报文结构

RADIUS 协议的报文结构如图 6-3 所示。

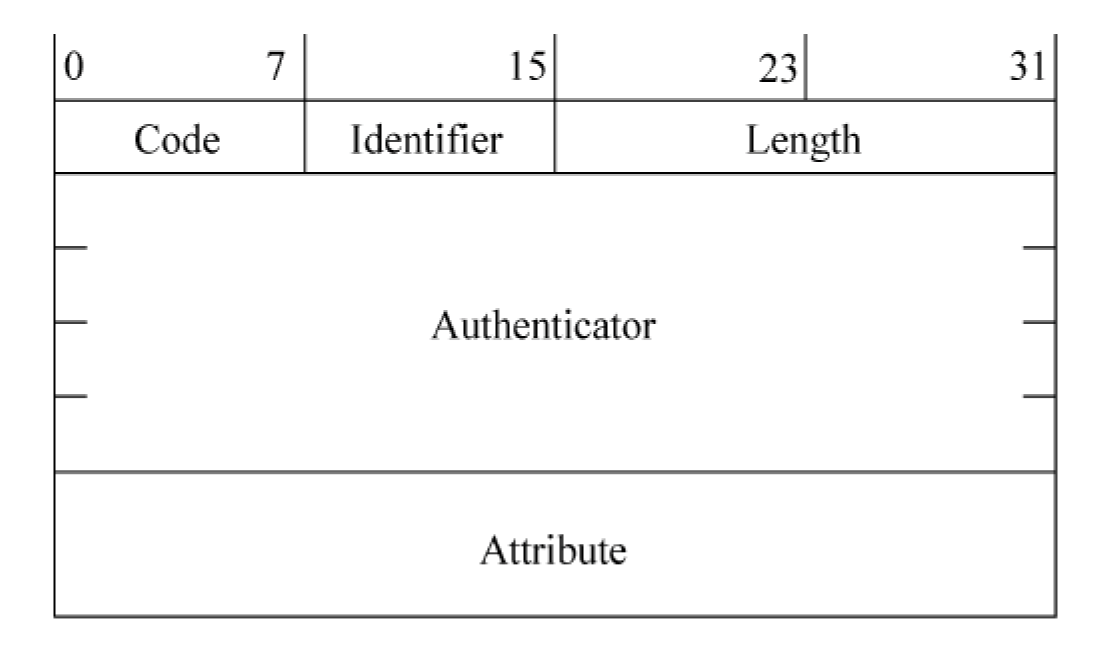


图 6-3　RADIUS 协议报文结构

RADIUS协议报文中的各项参数说明如下。

(1) Code：用于标识RADIUS报文的类型，长度为1个字节。RADIUS报文的类型如表6-1所示。

表6-1 RADIUS报文类型

Code	报文类型	报文说明
1	Access-Request	认证请求包，由RADIUS客户端发送往RADIUS服务器
2	Access-Accept	认证接受包，由RADIUS服务器发送往RADIUS客户端，表示认证通过
3	Access-Reject	认证拒绝包，由RADIUS服务器发送往RADIUS客户端，表示认证失败
4	Accounting-Request	计费请求包，由RADIUS客户端发送往RADIUS服务器，使用Acct-Status-Type属性值来区分计费开始请求和计费结束请求
5	Accounting-Response	计费响应包，由RADIUS服务器发送往RADIUS客户端，通知客户端已收到计费请求包并已经正确记录计费信息

(2) Identifier：用于匹配请求包和响应包，以及检测一段时间内重发的请求包，随着Attribute的改变以及接收到的有效响应包的变化而不断变化，而在重传时保持不变。长度为1个字节。

(3) Length：标识整个包的长度。超过长度域的字节被视为填充，在接收时会被忽略；而如果接收到的数据包短于Length标识的长度，则会被丢弃。长度为2个字节。

(4) Authenticator：用于验证RADIUS服务器的应答报文，以及对用户密码的加密计算。长度为16个字节。

(5) Attribute：携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。长度不定。该字段包含多个RADIUS属性，并采用TLV(Type、Length、Value)三元组的形式对属性进行描述。

① 类型(Type)：1个字节，取值为1～255，用于标识属性的类型。

② 长度(Length)：1个字节，标识此属性的长度，包括类型字段、长度字段和属性值字段。

③ 属性值(Value)：具体属性的取值，其格式和内容由类型域和长度域决定，最大长度为253字节。

3. RADIUS常见属性

RADIUS协议的标准属性有一百余个，常用到的一些属性如表6-2所示。

表6-2 RADIUS常用属性

属性编码	属性名称	属性描述
1	User-Name	需要进行认证的用户名称
2	User-Password	需要进行PAP方式认证的用户密码
3	CHAP-Password	需要进行CHAP方式认证的用户密码摘要

续表

属性编码	属 性 名 称	属 性 描 述
4	NAS-IP-Address	RADIUS 客户端的 IP 地址，默认情况下为客户端发送 RADIUS 报文的接口 IP 地址，建议配置固定的 NAS-IP-Address，以避免因为发送接口的变化而导致 NAS-IP 的变化
5	NAS-Port	用户接入 NAS 的物理端口号，由"槽位号＋端口号＋VLAN 号"构成
6	Service-Type	用户申请认证的业务类型
7	Framed-Protocol	固定为 1，表示 PPP 类型
8	Framed-IP-Address	用户的 IP 地址
14	Login-IP-Host	Login 登录用户的 IP 地址，但实际显示为 NAS 的 IP 地址
15	Login-Service	用户登录设备时采用的服务类型
26	Vendor-Specific	厂商自定义的私有属性，一个报文中可以有一个或多个私有属性，每个私有属性中可以有一个或多个子属性。例如，H3C 的管理员账号的管理级别即由相关的私有属性来实现
31	Calling-Station-ID	NAS 用于向 RADIUS 服务器告知标识用户的号码，在 LAN-Access 业务中，该字段填充的是用户的 MAC 地址；在 Login 中，该字段取值为全 0
32	NAS-Identifier	NAS 的主机名
40	Acct-Status-Type	标识计费请求报文的类型是开始计费、结束计费还是实时计费
44	Acct-Session-Id	计费的连接号，对于同一个连接的开始计费、实时计费和结束计费报文，其 Acct-Session-Id 必须相同
45	Acct-Authentic	用户的认证模式，1 表示 RADIUS 认证，2 表示本地认证
55	Event-Timestamp	生成计费报文的时间，以秒为单位，表示从 1970 年 1 月 1 日零点零分零秒以来的绝对秒数
60	CHAP-Challenge	CHAP 认证的质询字，只用于 CHAP 认证
61	NAS-Port-Type	NAS 的端口类型

6.2.2　RADIUS 的配置

RADIUS 的配置分为 RADIUS 客户端的配置和 RADIUS 服务器端的配置两部分，下面分别对其进行介绍。

1. RADIUS 客户端的配置

RADIUS 的客户端即作为 NAS 的网络设备。在 H3C 网络设备上配置 RADIUS 分为配置 RADIUS 方案和在 AAA 域中引用 RADIUS 方案两个步骤。

（1）配置 RADIUS 方案。

配置 RADIUS 方案涉及的命令如下。

① 创建 RADIUS 方案。

```
[H3C]radius scheme radius-scheme-name
```

一个 RADIUS 方案可以同时被多个 AAA 域引用。

② 配置主认证/授权服务器和备份认证/授权服务器。

```
[H3C-radius-login]primary authentication ip-address [port-number]
[H3C-radius-login]secondary authentication ip-address [port-number]
```

其中,端口号默认为1812。

③ 配置主计费服务器和备份计费服务器。

```
[H3C-radius-login]primary accounting ip-address [port-number]
[H3C-radius-login]secondary accounting ip-address [port-number]
```

其中,端口号默认为1813。

④ 配置网络设备的NAS-IP。

```
[H3C-radius-login]nas-ip ip-address
```

为保证认证的有效性和安全性,RADIUS服务器需要验证NAS的IP地址,只有在RADIUS服务器的NAS-IP地址列表范围内的认证请求才会被处理,否则将不予处理。默认情况下网络设备会以发送RADIUS报文的接口IP地址作为NAS-IP,但在多接口设备上很可能会因为发送接口的变化而导致NAS-IP的变化,从而最终导致认证的失败。因此建议配置确定的NAS-IP,以保证认证的正常进行。

⑤ 配置RADIUS报文的共享密钥。

```
[H3C-radius-login]key authentication string
[H3C-radius-login]key accounting string
```

共享密钥有两个功能,一方面RADIUS服务器和RADIUS客户端使用共享密钥来验证对方身份的合法性;另一方面共享密钥对RADIUS报文中传送的用户密码进行加密保护。只有在RADIUS服务器和RADIUS客户端配置的共享密钥相同的情况下,双方才能彼此接收对方发来的报文并作出相应。

⑥ 配置用户名的格式。

```
[H3C-radius-login]user-name-format {with-domain|without-domain}
```

由于在NAS上可能存在多个AAA域,而每一个AAA域可能会引用不同的RADIUS方案,因此用户发送给NAS的用户名往往需要携带有AAA域名信息,格式为"user-name@aaa-name",其中aaa-name即为用户所在AAA域的域名。在NAS接收到用户信息后,会根据用户名中的aaa-name信息判断用户归属于哪一个AAA域,然后使用该AAA域引用的RADIUS方案到相应的RADIUS服务器上进行认证。

在默认情况下,NAS发送给RADIUS服务器的用户名携带有AAA域名信息,但部分早期的RADIUS服务器不能识别带有AAA域名的用户名,此时就需要使用user-name-format without-domain命令指定NAS在给RADIUS服务器发送的用户名中去除掉AAA域名。

需要注意的是,如果在RADIUS方案中配置了不允许用户名携带AAA域名,则该RADIUS方案只能被一个AAA域引用。如果多个AAA域引用该RADIUS方案,则会

出现虽然实际用户不同(在不同的 AAA 域中)但 RADIUS 服务器认为用户相同(不携带 AAA 域名的用户名相同)的错误。

⑦ 配置定时器。

```
[H3C-radius-login]timer response-timeout seconds
[H3C-radius-login]timer quiet minutes
[H3C-radius-login]timer realtime-accounting minutes
```

3 个定时器从上到下分别是服务器响应超时定时器、主服务器恢复激活状态定时器和实时计费间隔定时器。

服务器响应超时定时器：用来控制 RADIUS 报文的超时重传,如果在 RADIUS 请求报文发送出去的时间已经到达服务器响应超时定时器规定的时间,但还没有收到来自 RADIUS 服务器的响应,则 NAS 就会重传 RADIUS 请求报文,以保证用户确实能够得到 RADIUS 服务。服务器响应超时定时器默认值为 3s。

主服务器恢复激活状态定时器：当主 RADIUS 服务器不可达时,状态变为 block,NAS 会与备份 RADIUS 服务器(如果配置了备份 RADIUS 服务器)进行交互,并开启定时器。在定时器时间到达主服务器恢复激活状态定时器规定的时间后,当有 RADIUS 请求时,NAS 会尝试与主 RADIUS 服务器通信,如果主 RADIUS 服务器恢复正常,则 NAS 会恢复与其通信,将其状态恢复为 active,并中断与备份 RADIUS 服务器的通信。主服务器恢复激活状态定时器默认值为 5min。

实时计费间隔定时器：同于对用户进行实时计费,每间隔一个实时计费间隔定时器规定的时间,NAS 就会向 RADIUS 服务器发送一次在线用户的计费信息。实时计费间隔定时器默认值为 12min。

⑧ 配置 RADIUS 报文超时重传次数。

```
[H3C-radius-login]retry retry-times
```

如果重传次数达到 retry 命令规定的值,而 NAS 仍未收到来自 RADIUS 服务器的响应,则本次 RADIUS 认证失败。默认超时重传次数为 3 次。

⑨ 配置 RADIUS 服务器类型。

```
[H3C-radius-login]server-type {extended|standard}
```

告诉 NAS 使用的 RADIUS 服务器是否支持私有属性的扩展,如果 RADIUS 服务器支持私有属性,则将 RADIUS 服务器类型配置为 extended;如果 RADIUS 服务器仅支持标准属性,则只能将 RADIUS 服务器类型配置为 standard。默认情况下 RADIUS 服务器的类型为 standard。

(2) 在 AAA 域中引用 RADIUS 方案。

配置了 RADIUS 方案后,需要在相应的 AAA 域中引用才能生效。在 AAA 域中引用 RADIUS 方案涉及的命令如下。

① 创建 AAA 域。

```
[H3C]domain domain-name
```

在大规模的网络应用中,不同 ISP 的用户有可能接入到同一台设备。而各 ISP 用户的用户属性(例如用户名及密码构成、服务类型/权限等)有可能不相同,因此有必要通过设置域来把它们区分开,并为每个域单独配置相应的 RADIUS 方案等属性集。各个域的控制相互独立,互不干扰。实际上,一个 AAA 域就是一个由属于同一个 ISP 用户构成的用户群。

系统默认存在一个名为 system 的 AAA 域。

② 配置域的认证方案。

[H3C-isp-teach]authentication {default|lan-access|login|portal|ppp|ssl-vpn|super|voip|wapi} {radius-scheme *radius-scheme-name* [local]|local|none}

lan-access、login、portal、ppp、ssl-vpn、super、voip 和 wapi 均为用户接入方式,AAA 可以对不同的接入方式和服务类型配置不同的认证方案。不同型号的设备对用户接入方式的支持情况也有所不同,上面命令中给出的是 H3C MSR 20-40 路由器支持的接入方式,在 H3C S3610 交换机中只支持 lan-access、login 和 super 3 种接入方式,而在 H3C E126A 交换机上则不能配置接入方式,在 authentication 后面直接配置 radius-scheme。

如果使用 default 参数,则配置的认证方案不区分用户类型,即对所有类型的用户都起作用,但此配置的优先级低于具体接入方式的配置。

如果配置了 radius-scheme *radius-scheme-name* local,则在 RADIUS 服务器没有响应时将使用本地认证。如果 local 或者 none 作为第一认证方案,则只能采用本地认证或者不进行认证,不能同时再采用 RADIUS 认证。

需要注意的是,对于 AAA 而言,认证、授权和计费是 3 个完全独立的业务流程,只是在 AAA 框架中使用的 RADIUS 协议将认证和授权绑定在了一起。因此当 RADIUS 被配置选择为认证方案时,AAA 只接受 RADIUS 服务器的认证结果,RADIUS 的授权信息虽然在认证接受包中被携带,但在认证回应的处理流程中不会被处理。

系统默认的域认证方案为 Local。

③ 配置域的授权方案。

[H3C-isp-teach]authorization {default|lan-access|login|portal|ppp|ssl-vpn|voip|wapi} {radius-scheme *radius-scheme-name* [local]|local|none}

参数含义与配置域的认证方案命令中的参数含义基本相同。

需要注意的是,对于 RADIUS 而言由于授权信息被包含在认证接受包中,因此必须将认证和授权的 RADIUS 方案配置相同,授权才起作用,否则系统会给出错误提示。但在有些设备中,例如,H3C E126A 中则不能配置引用 RADIUS 方案的授权,只需要配置认证方案即可。

系统默认的域授权方案为 Local。

④ 配置域的计费方案。

[H3C-isp-teach]accounting {default|lan-access|login|portal|ppp|ssl-vpn|voip|wapi} {radius-scheme *radius-scheme-name* [local]|local|none}

参数含义与配置域的认证方案命令中的参数含义基本相同。

系统默认的域计费方案为 Local。

⑤ 配置计费可选。

```
[H3C-isp-teach]accounting optional
```

在对用户实施计费时,如果发现没有可用的计费服务器或与计费服务器通信失败,则用户连接将被挂断;但如果配置了 accounting optional 命令,则即使计费失败,用户依然可以继续使用网络资源。

⑥ 配置默认域。

```
[H3C]domain default enable domain-name
```

NAS 需要根据用户名中携带的域名信息来判断用户所在的 AAA 域,进而使用该 AAA 域引用的 RADIUS 方案到相应的 RADIUS 服务器上进行认证。但如果用户发送的用户名中不包含域名信息,则系统将使用默认的域进行认证。

默认情况下,系统默认域是 system。

在 Cisco 设备上配置 RADIUS 涉及的命令如下。

(1) 配置 RADIUS 服务器。

```
Router(config)# radius-server host ip-address [auth-port port-number] [acct-port port-number]
```

其中,参数 *ip-address* 是 RADIUS 服务器的 IP 地址,参数 auth-port 和 acct-port 分别用来指定认证和授权、计费使用的 UDP 端口号。

(2) 配置 RADIUS 报文的共享密钥。

```
Router(config)# radius-server key key-string
```

(3) 配置 RADIUS 服务器的响应超时时间。

```
Router(config)# radius-server timeout seconds
```

Cisco 设备上 RADIUS 服务器的默认响应超时时间为 5s。

(4) 配置 RADIUS 报文超时重传次数。

```
Router(config)# radius-server retransmit retry-times
```

Cisco 设备上默认的超时重传次数与 H3C 设备上相同,均为 3 次。

(5) 开启 AAA 功能。

```
Router(config)# aaa new-model
```

在 Cisco 设备上,AAA 安全特性默认处于关闭状态,在配置之前,首先要开启该功能。

(6) 配置 AAA 的认证方法。

```
Router(config)# aaa authentication {login|ppp|enable} {default|list-name} method1 [method2...]
```

其中,参数 *list-name* 为方法列表名称,在指定 AAA 的认证方法时,可以使用 default 参数指定某一个或几个认证方法为默认的认证方法;也可以使用 *list-name* 参数为某一个或几个认证方法指定一个唯一的方法列表名称。其中默认的认证方法会被应用在所有线路上,而如果某一条线路需要使用特定方法列表定义的认证方法,则需要在线路配置模

式下使用 login authentication *list-name* 命令来指定。

参数 *method* 为具体的认证方法,其中 login 认证可用的认证方法如表 6-3 所示。

表 6-3 Cisco 设备 login 可用的认证方法

认证方法	描　　述
enable	使用 enable 口令进行认证
line	使用用户正在试图访问的线路上的 password 进行认证
local	使用本地数据库中的用户名和口令进行认证(不区分大小写)
local-case	使用本地数据库中的用户名和口令进行认证(区分大小写)
none	不进行认证
group radius	使用 radius-server 命令定义的 RADIUS 服务器进行认证
group tacacs+	使用 tacacs-server 命令定义的 TACACS+服务器进行认证

在一个认证方法列表中,最多可以列出 4 种方法,当前面的认证方法认证失败后,将使用下一个认证方法进行认证。

(7) 配置 AAA 的授权方法。

```
Router(config)#aaa authorization type {default|list-name} method1 [method2...]
```

其中,参数 *type* 表示授权类型,即对哪一类权限进行授权控制。在 Cisco 设备上可用的授权类型如表 6-4 所示。

表 6-4 Cisco 设备可用的授权类型

授权类型	描　　述
auth-proxy	在每个用户基础上应用指定的安全策略
exec	用于与用 EXEC 终端会话相关属性的授权
network	用于对用户的网络连接(PPP、SLIP、ARAP)进行相应的授权
commands	用于对 EXEC 命令级别进行授权
configuration	用于从 AAA 服务器上下载配置的授权
ipmobile	用于对 IP 移动服务的授权
reverse-access	用于对反向 Telnet 会话的授权

参数 *method* 为具体的授权方法,包括 local、none、group radius、group tacacs+以及 if-authenticated。其中,if-authenticated 为允许已经成功验证的用户访问所请求的功能。

(8) 配置 AAA 的计费方法。

```
Router(config)#aaa accounting type {default|list-name} {start-stop|stop-only|none} method1
[method2...]
```

其中,参数 start-stop 表示在事件开始和结束时分别建立计费记录;stop-only 表示只在事件结束时建立一个计费记录;none 表示关闭相应事件的计费记录。

(9) 在特定的线路上应用认证、授权和计费。

```
Router(config-line)#login authentication {default|list-name}
Router(config-line)#authorization type {default|list-name}
Router(config-line)#accounting type {default|list-name}
```

2. RADIUS 服务器端的配置

RADIUS 服务器负责集中管理用户信息，对用户进行认证、授权和计费。RADIUS 服务器通常需要维护 3 个数据库：Users、Clients 和 Dictionary。

Users：用于存储用户信息，例如用户名、密码等。

Clients：用于存储 RADIUS 客户端的信息，例如 NAS 的 IP 地址、共享密钥等。

Dictionary：用于存储 RADIUS 的属性和属性值与其数字 ID 的对应关系，以及每个属性所允许的数据类型等。

在这里使用一款免费的 RADIUS 服务器软件 FreeRADIUS.net 来搭建 RADIUS 服务器。该软件可以去其官方网站 http://www.freeradius.net 下载。

（1）FreeRADIUS.net 的安装

FreeRADIUS.net 的安装非常简单，具体如图 6-4～图 6-7 所示。



图 6-4　FreeRADIUS.net 安装欢迎界面

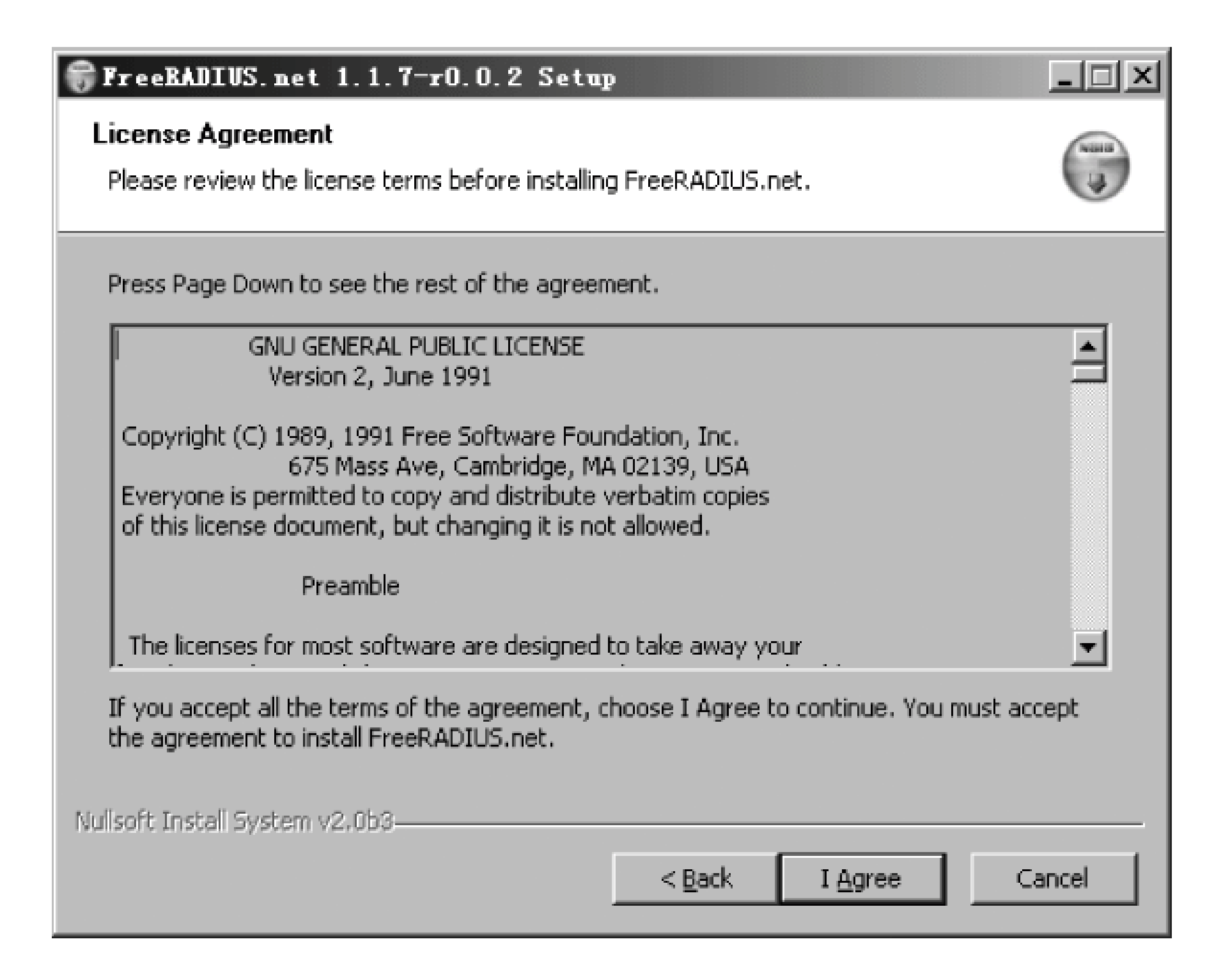


图 6-5　FreeRADIUS.net 版权信息界面

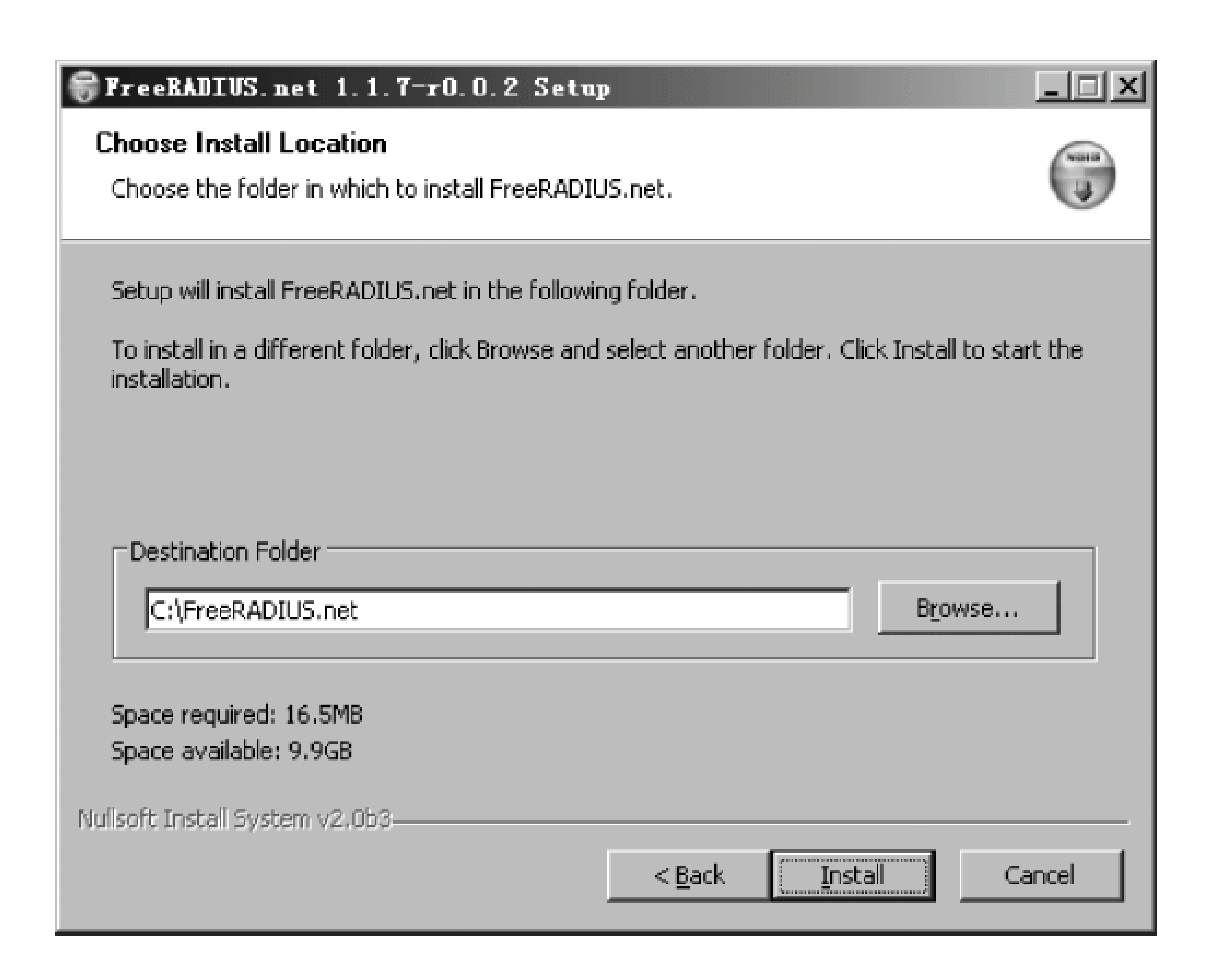


图 6-6 FreeRADIUS. net 安装路径界面

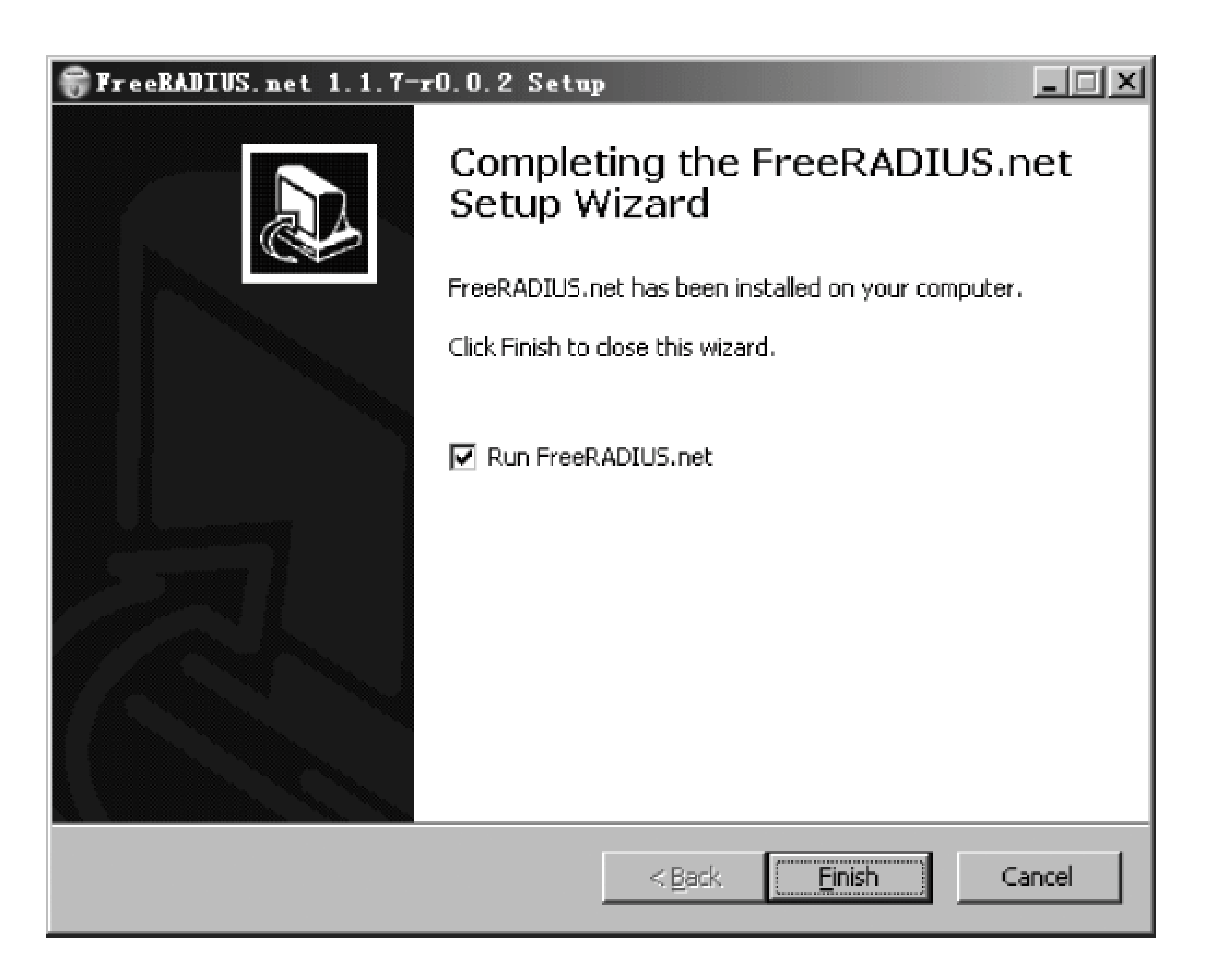


图 6-7 FreeRADIUS. net 安装完成界面

安装完成后，运行 FreeRADIUS. net，在命令行界面下输入 netstat-an 命令查看系统端口监听情况，可以看到 UDP 的 1812 和 1813 两个端口处于监听状态。

(2) FreeRADIUS. net 的配置

FreeRADIUS. net 在安装后必须要经过配置才能够正常工作。FreeRADIUS. net 的配置文件均保存在其安装目录下的 etc\raddb 子目录中。配置主要涉及 clients. conf 和 users. conf 两个配置文件。

① 配置 RADIUS 客户端信息。RADIUS 客户端信息在配置文件 clients. conf 中进行配置。使用写字板打开 clients. conf 文件，并在文件末尾为每一个 RADIUS 客户端添加一段配置信息如下：

```
client RADIUS 客户端 IP 地址/网络前缀{
```

```
        secret         = RADIUS 服务器与 RADIUS 客户端的共享密钥值
        shortname      = RADIUS 客户端的主机名
}
```

其中，shortname 可以是任意值，并不要求一定要和 RADIUS 客户端的主机名一致。

② 配置 RADIUS 用户信息。RADIUS 用户信息在配置文件 users.conf 中进行配置。使用写字板打开 users.conf 文件，并在文件最开始的位置为每一个用户添加一行配置信息如下：

```
用户名    User-Password == "用户密码"
```

其中，用户名是否携带 AAA 域名需要和 RADIUS 客户端上的 user-name-format 命令的配置一致。

注意： 在配置完成后，必须重启 FreeRADIUS 服务，配置才能够生效。

3. RADIUS 配置举例

假设存在如图 6-8 所示的网络，要求配置 RADIUS 服务，使 PC_1 远程登录到交换机上时首选使用 RADIUS 进行认证、授权和计费，在 RADIUS 服务器没有响应时则使用本地认证、授权和计费。其中要求配置 AAA 域名为 network，RADIUS 服务器与 RADIUS 客户端之间的共享密钥为 computer，RADIUS 认证使用的用户名和密码分别是 abc 和 123，本地认证使用的用户名和密码分别是 xyz 和 456。

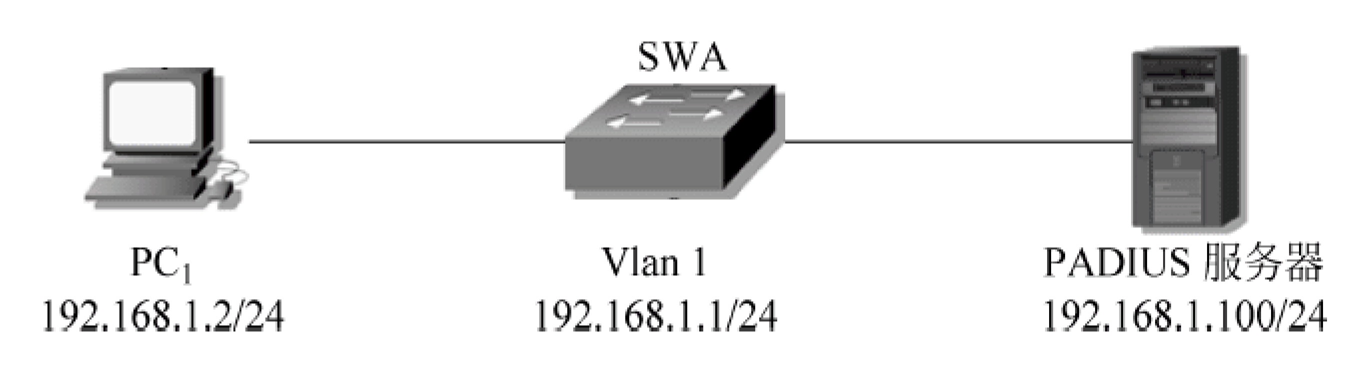


图 6-8　RADIUS 的配置

H3C 交换机上具体的配置命令如下：

```
[SWA]user-interface vty 0 4
[SWA-ui-vty0-4]authentication-mode scheme
[SWA-ui-vty0-4]quit
[SWA]local-user xyz
[SWA-luser-xyz]password simple 456
[SWA-luser-xyz]level 3
[SWA-luser-xyz]service-type telnet
[SWA-luser-xyz]quit
[SWA]radius scheme login
[SWA-radius-login]primary authentication 192.168.1.100
[SWA-radius-login]primary accounting 192.168.1.100
[SWA-radius-login]nas-ip 192.168.1.1
[SWA-radius-login]key authentication computer
[SWA-radius-login]key accounting computer
[SWA-radius-login]user-name-format with-domain
[SWA-radius-login]server-type standard
```

```
[SWA-radius-login]quit
[SWA]domain network
[SWA-isp-network]authentication radius-scheme login local
[SWA-isp-network]accounting radius-scheme login
[SWA-isp-network]accounting optional
[SWA-isp-network]quit
[SWA]domain default enable network
```

注意:在这里使用的交换机是 H3C E126A,配置命令与本节的第一小节中给出的配置命令存在部分区别。另外,由于 FreeRADIUS 不支持 H3C 的私有属性,因此服务器类型被设置为 standard。

Cisco 交换机上具体的配置命令如下:

```
SWA(config)#username xyz password 456
SWA(config)#aaa new-model
SWA(config)#radius-server host 192.168.1.100 auth-port 1812 acct-port 1813
SWA(config)#radius-server key computer
SWA(config)#aaa authentication login tel-authen group radius local
SWA(config)#aaa accounting connection tel-acc start-stop group radius
SWA(config)#line vty 0 4
SWA(config-line)#login authentication tel-authen
SWA(config-line)#accounting connection tel-acc
```

注意:Cisco 交换机上没有关于域名 network 的配置命令。

RADIUS 服务器的配置如下:

配置文件 clients.conf 的末尾添加如下信息:

```
client 192.168.1.1/24 {
        secret          = computer
        shortname       = SWA
}
```

配置文件 users.conf 的开始位置添加如下信息:

```
abc@network     User-Password == "123"
```

注意:如果是 H3C 交换机,配置文件 users.conf 中的用户名为 abc@network;而如果是 Cisco 交换机,配置文件 users.conf 中的用户名为 abc。

配置完成后,重新启动 FreeRADIUS 服务。

在 PC_1 的命令行界面下使用 Telnet 命令登录交换机 SWA,同时在 RADIUS 服务器上打开 Wireshark 软件捕获数据包。

如果交换机 SWA 为 H3C 设备,PC_1 上的登录信息如下:

```
C:\Documents and Settings\Administrator>telnet 192.168.1.1

Login authentication

Username:abc
```

```
Password:
<SWA>
%Apr  2 00:40:58:059 2000 SWA SHELL/5/LOGIN:- 1 - abc(192.168.1.2) in unit1 login
<SWA>system-view
        ^
% Unrecognized command found at '^' position.
<SWA>quit
```

从 PC_1 上的登录信息可以看出，使用用户名 abc 成功登录到交换机 SWA，该用户的登录是使用 RADIUS 服务器进行认证实现的。由于 FreeRADIUS 服务不支持 H3C 的私有属性，无法对用户的级别进行分级授权，因此用户 abc 在登录到交换机 SWA 上后只具有默认的最低访问级的权限。

如果交换机 SWA 为 Cisco 设备，PC_1 上的登录信息如下：

```
C:\Documents and Settings\Administrator>telnet 192.168.1.1

User Access Verification

Username:abc
Password:
SWA>enable
SWA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWA(config)#
```

在 RADIUS 服务器上捕获的 Wireshark 数据包如图 6-9 所示。

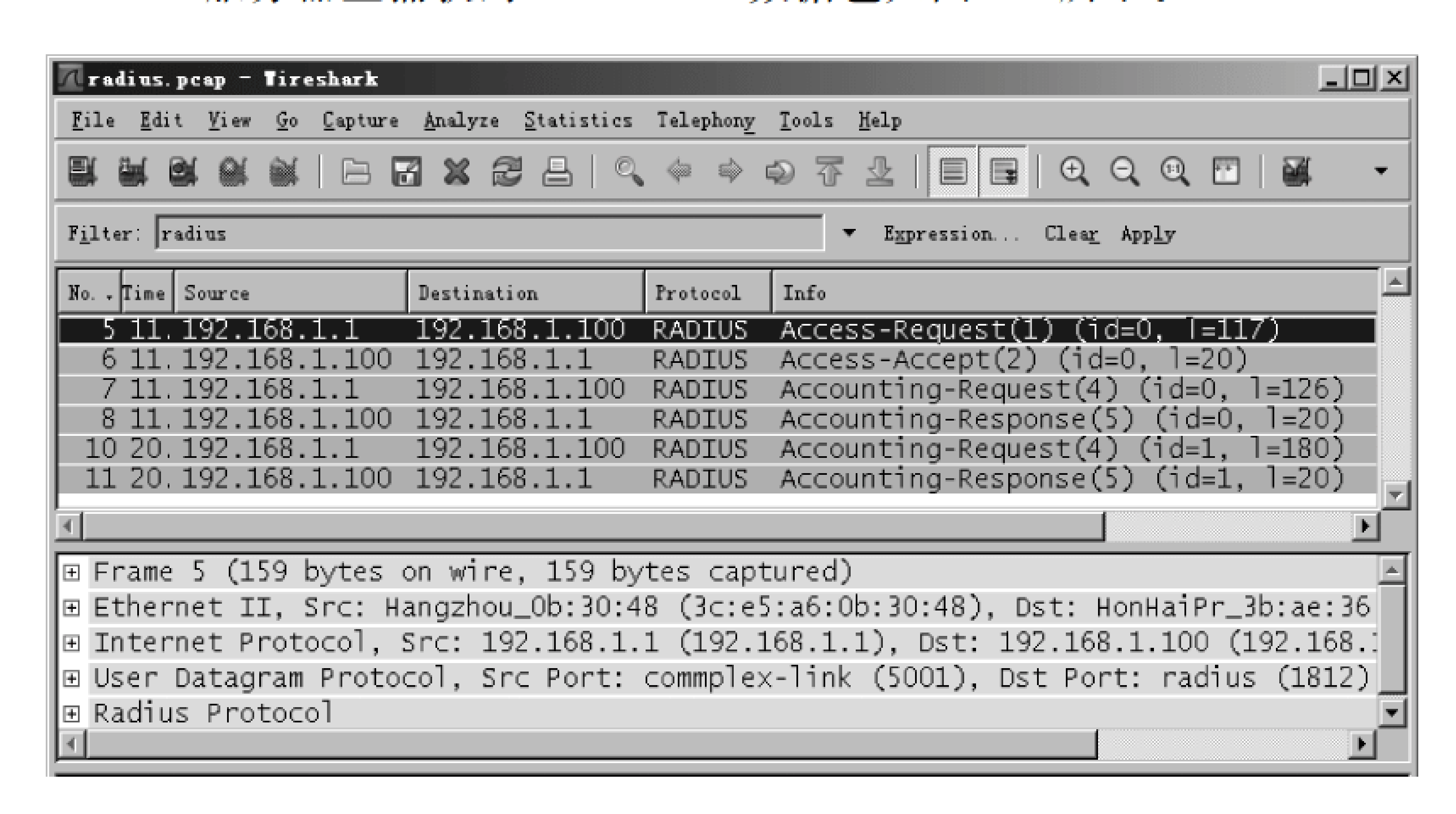


图 6-9　RADIUS 数据报文

从上图中可以看到 RADIUS 的认证请求包、认证接受包、计费开始请求包、计费开始请求响应包、计费结束请求包和计费结束请求响应包。

此时使用用户名 xyz 无法登录到交换机 SWA 上，因为 RADIUS 服务器上的配置文件 users.conf 中不存在用户名 xyz 的信息。

将 RADIUS 服务器 DOWN 掉，然后在 PC_1 的命令行界面下使用 Telnet 命令登录交

换机 SWA,将会发现用户名 abc 无法登录到交换机 SWA 上,但用户名 xyz 则可以登录。具体信息如下:

```
C:\Documents and Settings\Administrator>telnet 192.168.1.1

Login authentication

Username:abc
Password:
% Login failed!

Username:xyz
Password:
<SWA>
%Apr  2 01:05:53:401 2000 SWA SHELL/5/LOGIN:- 1 - xyz(192.168.1.2) in unit1 login
<SWA>system-view
System View: return to User View with Ctrl+Z.
[SWA]
```

这是因为在 AAA 域配置了 Local 为第二认证方案,因此在 RADIUS 服务器 DOWN 掉以后,将使用本地认证。由于在本地用户 xyz 的配置中指定了其运行级别为管理级,因此用户 xyz 登录到交换机 SWA 上以后,将被授权拥有管理级的权限。

RADIUS 服务器对用户进行认证后,会在 FreeRADIUS.net 的安装目录下的 var\log\radius\radacct 子目录中保存认证和计费信息。FreeRADIUS 会为每一个 NAS 建立一个以 NAS 的 IP 地址命名的子目录,在该子目录中包含 3 个文件,分别是:auth-detail-日期.log、detail-日期.log 和 reply-detail-日期.log。

文件"auth-detail-日期.log"保存的是用户认证信息,具体内容如下:

```
Packet-Type = Access-Request
Sat Feb 11 03:53:40 2012
    User-Name = "abc@network"
    User-Password = "123"
    NAS-IP-Address = 192.168.1.1
    NAS-Identifier = "3ce5a60b3048"
    NAS-Port = 16838657
    NAS-Port-Type = Ethernet
    Service-Type = Login-User
    Login-IP-Host = 192.168.1.1
    Calling-Station-Id = "0000-0000-0000"
    Framed-IP-Address = 192.168.1.2
    Client-IP-Address = 192.168.1.1
```

文件"detail-日期.log"保存的是用户计费信息,具体内容如下:

```
Sat Feb 11 03:53:40 2012
    User-Name = "abc@network"
    NAS-Identifier = "3ce5a60b3048"
    NAS-Port = 16838657
```

```
    NAS-Port-Type = Ethernet
    Calling-Station-Id = "0000-0000-0000"
    Acct-Status-Type = Start
    Acct-Authentic = RADIUS
    Acct-Session-Id = "1100030201406"
    Framed-IP-Address = 192.168.1.2
    NAS-IP-Address = 192.168.1.1
    Event-Timestamp = "Apr  2 2000 09:40:26"
    Service-Type = Login-User
    Client-IP-Address = 192.168.1.1
    Acct-Unique-Session-Id = "96ed5f593923a615"
    Timestamp = 1328903620

Sat Feb 11 03:53:45 2012
    User-Name = "abc@network"
    NAS-Identifier = "3ce5a60b3048"
    NAS-Port = 16838657
    NAS-Port-Type = Ethernet
    Calling-Station-Id = "0000-0000-0000"
    Acct-Status-Type = Stop
    Acct-Authentic = RADIUS
    Acct-Session-Id = "1100030201406"
    Framed-IP-Address = 192.168.1.2
    NAS-IP-Address = 192.168.1.1
    Event-Timestamp = "Apr  2 2000 09:40:31"
    Service-Type = Login-User
    Acct-Session-Time = 5
    Acct-Delay-Time = 0
    Acct-Input-Octets = 0
    Acct-Input-Packets = 0
    Acct-Output-Octets = 0
    Acct-Output-Packets = 0
    Acct-Input-Gigawords = 0
    Acct-Output-Gigawords = 0
    Acct-Terminate-Cause = NAS-Error
    Client-IP-Address = 192.168.1.1
    Acct-Unique-Session-Id = "96ed5f593923a615"
    Timestamp = 1328903625
```

文件“reply-detail-日期.log”的具体内容如下：

```
Packet-Type = Access-Accept
Sat Feb 11 03:53:40 2012
```

6.3　IEEE 802.1x

在以太网中，默认情况下用户主机只要可以连接到交换机的物理端口，就可以访问整个网络中的所有资源。但是在商务以太网(如写字楼中的以太网)或移动办公等应用场

合,网络服务的提供者往往希望对终端用户的接入进行控制,即在以太网接入设备的端口一级对所接入的设备进行认证和控制,从而产生了基于端口的网络接入控制(Port Based Network Access Control)需求。在网络中,实现这一需求的协议为 IEEE 802.1x。

IEEE 802.1x 协议最初作为无线局域网的接入控制协议出现,用来解决无线局域网用户的接入认证问题,后来被引入到有线局域网中进行用户接入认证。在应用了 IEEE 802.1x 的交换机端口上,如果该端口连接的终端设备能够通过认证,即可以访问网络中的资源;而如果不能通过认证,则无法访问网络中的资源。

6.3.1 IEEE 802.1x 的体系结构

IEEE 802.1x 采用 C/S 结构,在其体系结构中包含客户端(Supplicant System)、设备端(Authenticator System)和认证服务器(Authentication Server System)3 个实体,具体如图 6-10 所示。

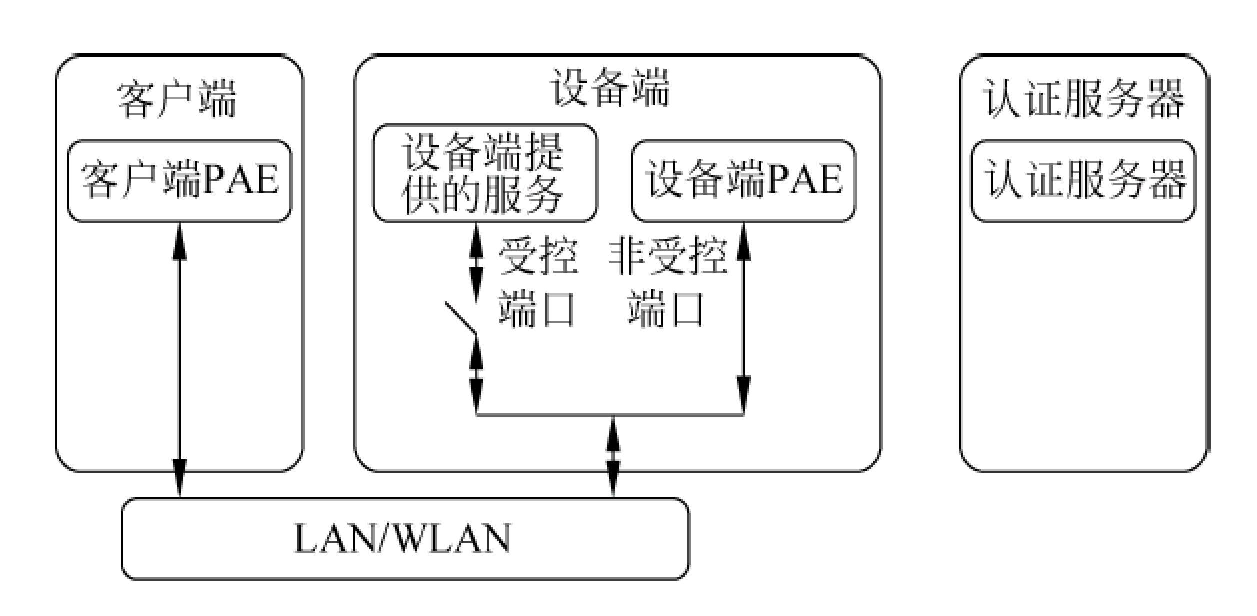


图 6-10 IEEE 802.1x 的体系结构

客户端是位于局域网一端的实体,由该链路另一端的设备端对其进行认证。客户端一般为 PC,通过启动 IEEE 802.1x 客户端软件发起 802.1x 认证,客户端需要支持局域网上的可扩展认证协议(Extensible Authentication Protocol Over LAN,EAPOL)。

设备端是位于局域网另一端的实体,用于对所连接的客户端进行认证。设备端一般为接入交换机,它为客户端提供接入局域网的端口,该端口可以是物理端口,也可以是逻辑端口。

认证服务器是为设备端提供认证服务的实体,用于实现对客户端的认证、授权和计费,一般是 RADIUS 服务器。

从图 6-10 中可以看到在客户端和设备端实体中有 PAE、受控端口和非受控端口,下面分别对其概念进行解释。

(1) PAE:PAE 的全称为 Port Access Entity,即端口访问实体。PAE 是在设备端口上具体负责执行算法和协议操作的实体对象。设备端 PAE 利用认证服务器对需要接入局域网的客户端进行认证,并根据认证结果来控制受控端口的状态为授权或者非授权;客户端 PAE 负责响应设备端的认证请求,向设备端提交用户的认证信息,客户端 PAE 也可以主动向设备端发送认证请求和下线请求。

(2) 受控端口和非受控端口:设备端为客户端提供的物理接入端口在逻辑上被划分成两个端口,即受控端口和非受控端口。作为同一个物理端口的两个部分,所有到达该物理端口的数据帧,在受控端口和非受控端口上均可见,但两个逻辑端口在功能实现上有所

区别。其中非受控端口始终处于双向联通状态，主要用来传递 EAPOL 协议帧，以保证客户端任何时候都能够发送或接收认证报文；受控端口则只有在授权状态下才处于联通状态，用于传递业务报文。

6.3.2　可扩展认证协议

可扩展认证协议(Extensible Authentication Protocol，EAP)在 IEEE 802.1x 认证系统中被用来在客户端、设备端和认证服务器之间交换认证信息。其中在客户端 PAE 和设备端 PAE 之间，EAP 协议报文使用 EAPOL 进行封装，直接承载于以太网环境中；而在设备端 PAE 和认证服务器之间则可以承载于 RADIUS 协议中，如图 6-11 所示。

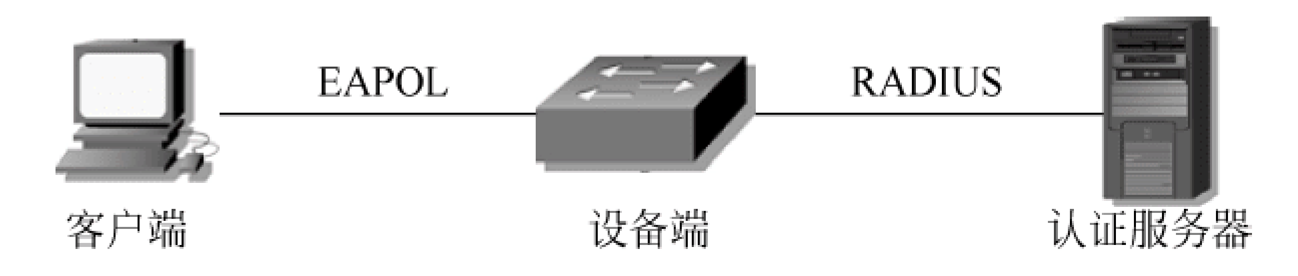


图 6-11　IEEE 802.1x 工作机制

1. EAPOL 报文结构

EAPOL 通过对 EAP 报文进行封装，使其可以在以太网上进行传送。EAPOL 的报文结构如图 6-12 所示。

EAPOL 报文中的各项参数说明如下。

(1) PAE Ethernet Type：表示协议类型，IEEE 802.1x 分配的协议类型为 0x888E。长度为 2 字节。

(2) Protocol Version：表示协议的版本号，长度为 1 字节。

(3) Type：表示 EAPOL 数据帧的类型，长度为 1 字节。EAPOL 数据帧的类型如表 6-5 所示。

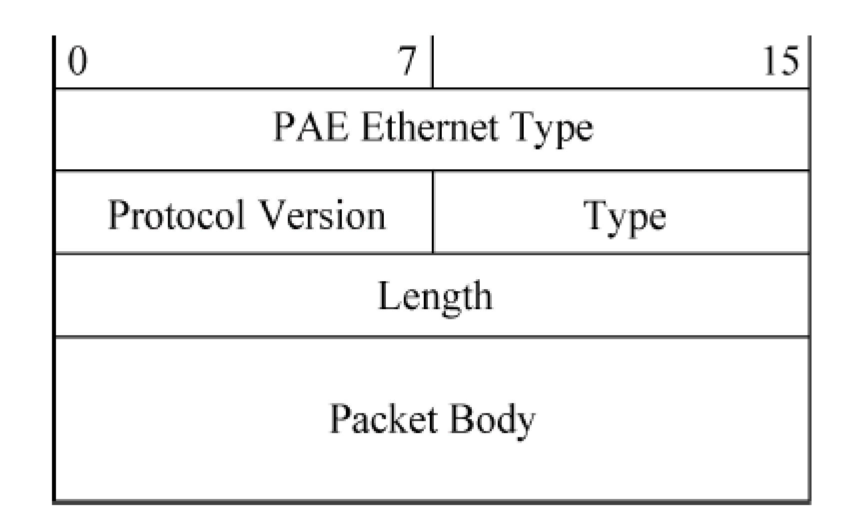


图 6-12　EAPOL 报文结构

表 6-5　EAPOL 数据帧的类型

Type	报 文 类 型	报 文 说 明
0	EAP-Packet	认证信息帧，用来承载认证信息
1	EAPOL-Start	认证发起帧
2	EAPOL-Logoff	退出请求帧

其中，EAPOL-Start 和 EAPOL-Logoff 报文中不包含 Packet Body 字段。

(4) Length：表示 Packet Body 字段的长度，单位为字节。EAPOL-Start 和 EAPOL-Logoff 报文中的 Length 字段取值为 0。长度为 2 字节。

(5) Packet Body：表示 EAP 报文内容，不同类型的 EAPOL 数据帧具有不同的格式。

2. EAP 报文结构

EAP-Packet 报文中的 Packet Body 部分即为 EAP 报文，其报文结构如图 6-13 所示。

EAP 报文中的各项参数说明如下。

(1) Code：表示 EAP 报文的类型，共有 4 种，分别是：Request、Response、Success 和 Failure。长度为 1 个字节。

(2) Identifier：用于匹配 Request 消息和 Response 消息，长度为 1 个字节。

(3) Length：EAP 报文的长度，包括 Code、Identifier、Length 和 Data 的全部内容，单位为字节。其取值与 EAPOL 报文中的 Length 字段的取值相同。长度为 2 个字节。

(4) Data：EAP 的数据信息，其中 Success 和 Failure 类型的 EAP 报文中没有 Data 字段；Request 和 Response 类型的 EAP 报文中的 Data 字段格式如图 6-14 所示。

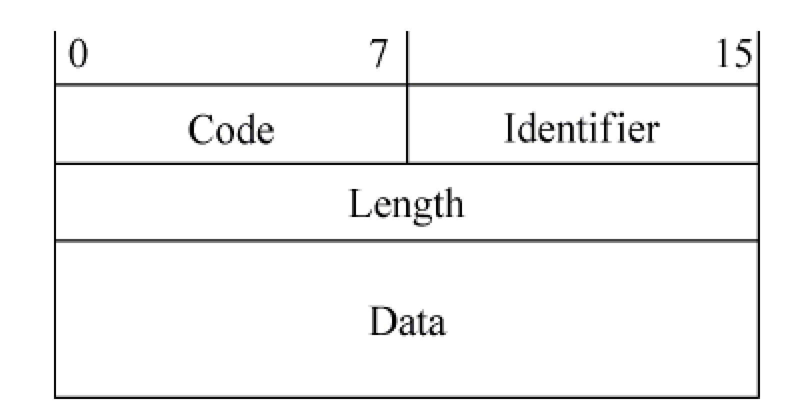


图 6-13　EAP 报文结构

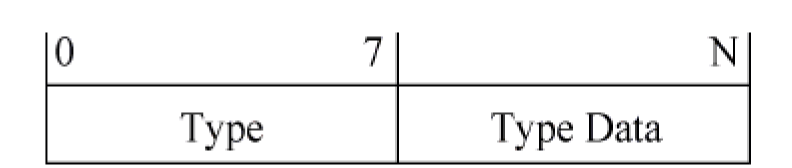


图 6-14　Data 字段格式

其中，Type 字段表示 EAP 的认证类型，取值为 1 时代表 Identity，用来查询对方的身份；取值为 4 时代表 MD5-Challenge，类似于 PPP 的 CHAP 协议，包含质询消息。Type Data 字段的内容由 Type 字段来决定，不同 EAP 认证类型的 Type Data 字段的取值不同。

6.3.3　IEEE 802.1x 本地认证

与 AAA 类似，IEEE 802.1x 也可以分为本地认证和远端认证两种方式，采用本地认证时，认证服务器集成在设备端上，即具体的用户名和密码信息均保存在设备端上。本地认证方式适用于网络规模较小、客户端数量不多的情况。

1. 本地认证流程

本地认证的具体流程如图 6-15 所示。

(1) 在用户有访问网络的需求时，打开 IEEE 802.1x 客户端程序输入用户名和密码，客户端程序向设备端发送 EAPOL-Start 报文，开始启动一次认证过程。

注意：EAPOL-Start 报文中不包含任何的 EAP 信息。

(2) 设备端收到来自客户端的 EAPOL-Start 报文后，向客户端发出 EAP-Request/Identity 报文，要求客户端发送输入的用户名，来查询客户端的身份。

(3) 客户端响应设备端的用户身份查询请求，将用户名信息通过 EAP-Response/Identity 报文发送给设备端。

(4) 设备端收到客户端发来的 EAP-Response/Identity 报文后，将其中的用户名信息与自己本地数据库中的用户名进行比对，找到该用户名对应的密码，并使用随机生成的一个加密字对密码进行加密处理，同时将随机加密字通过 EAP-Request/MD5-Challenge 报文发送给客户端。

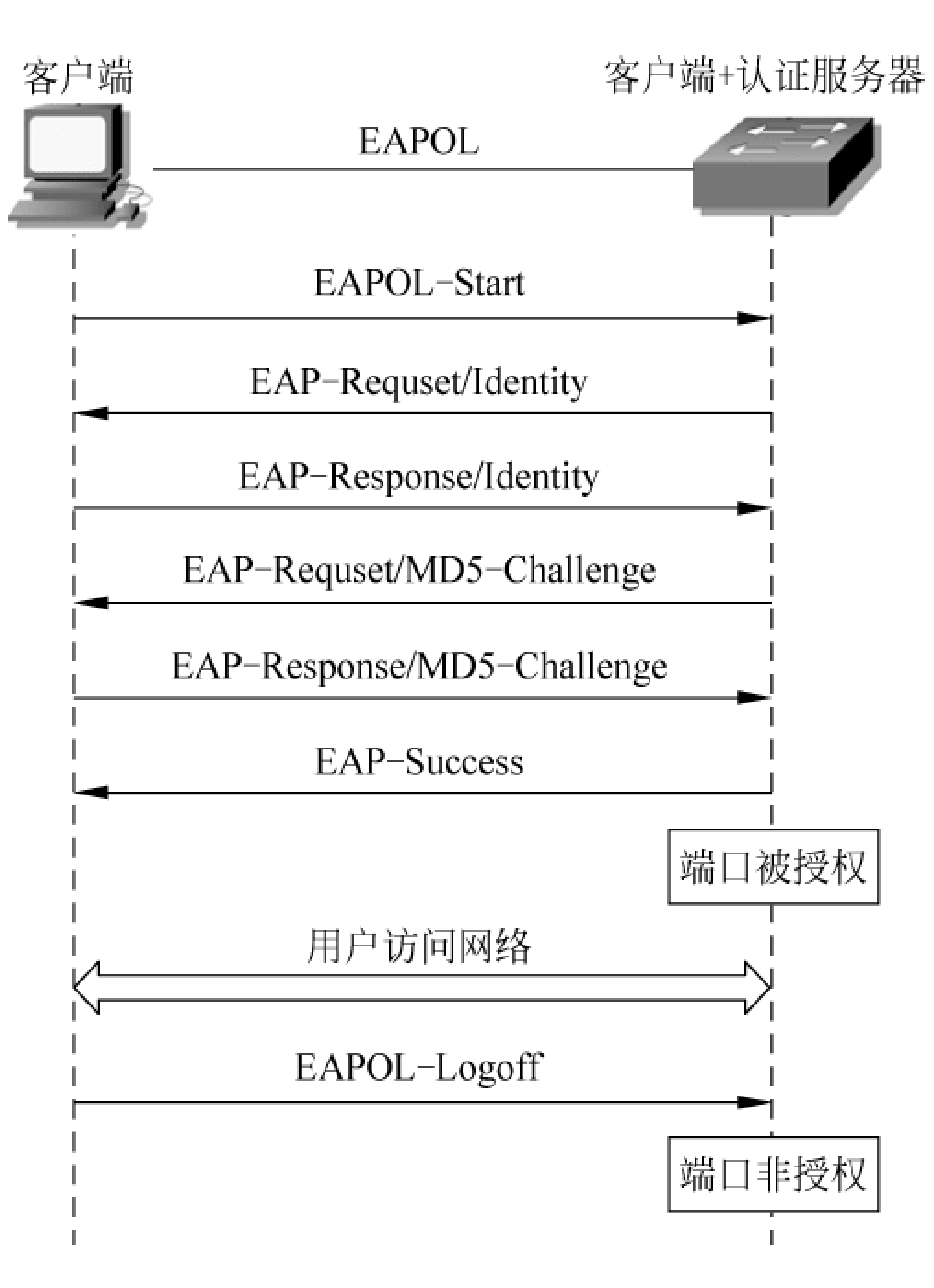


图 6-15　IEEE 802.1x 本地认证流程

(5) 客户端收到设备端发来的 EAP-Request/MD5-Challenge 报文后,使用其中的随机加密字对密码进行加密处理,并将加密后的密码通过 EAP-Response/MD5-Challenge 报文发送给设备端。

(6) 设备端将从客户端发来的 EAP-Response/MD5-Challenge 报文中获得的加密密码与自己计算出的加密密码进行比对,若两者相同,则认为用户合法。向客户端发送 EAP-Success 报文,通知客户端 IEEE 802.1x 认证通过,同时将受控端口的状态改为授权状态,允许用户通过该端口访问网络。

(7) 用户下线时,客户端向设备端发送 EAPOL-Logoff 报文,设备端将受控端口的状态由授权状态改为非授权状态,不再允许用户通过该端口访问网络。

2. 本地认证配置

IEEE 802.1x 本地认证的配置分为设备端的配置和客户端的配置两部分,下面分别对其进行介绍。

(1) H3C 设备端的配置

① 开启全局的 IEEE 802.1x 特性。

```
[H3C]dot1x
```

在默认情况下,网络设备上不启用 IEEE 802.1x 功能。

② 开启相应端口的 IEEE 802.1x 特性。

```
[H3C-Ethernet1/0/1]dot1x
```

在默认情况下，所有端口的 IEEE 802.1x 特性均为关闭状态，必须要同时开启全局和端口的 IEEE 802.1x 特性后，IEEE 802.1x 的配置才会在相应端口上生效。因此在同一台网络接入设备上可以配置一部分端口连接的用户需要进行 IEEE 802.1x 认证，而另一部分可以直接访问网络，增加了其应用的灵活性。

③ 添加本地用户信息。

```
[H3C]local-user user-name
[H3C-luser-user-name]password {simple|cipher} password
    [H3C-luser-user-name]service-type lan-access
```

注意：本地用户的服务类型必须为 lan-access，即局域网接入。

④ 关闭在线用户握手功能。

```
[H3C]undo dot1x handshake enable
```

在 H3C 的网络设备上，默认开启在线用户握手功能，即在用户认证成功后设备端每隔一定的时间(默认为 15s)就会向客户端发送握手请求报文 EAP-Request/Identity，来定期检测用户的在线情况，客户端需要使用握手回应报文 EAP-Response/Identity 进行响应。该功能需要有 H3C 私有客户端的支持，而对于非 H3C 客户端，由于其不会向设备端发送握手回应报文，因此设备端将会错误地认为用户已经下线。所以如果使用的是非 H3C 客户端，一定要在设备端关闭在线用户握手功能。

⑤ 设置端口接入控制方式。

```
[H3C-Ethernet1/0/1]dot1x port-method {macbased|portbased}
```

H3C 的网络设备支持两种不同的接入控制方式。

基于端口的接入控制方式：只要某物理端口下的第一个用户认证成功后，该端口下的其他接入用户无需认证就可以访问网络，但当第一个用户下线后，其他用户也会被拒绝访问网络。

基于 MAC 地址的接入控制方式：同一端口下的所有接入用户都需要单独认证，在某个用户下线时，不影响其他用户访问网络。

默认接入控制方式为基于 MAC 地址的接入控制方式。

(2) Cisco 设备端的配置

① 定义 IEEE 802.1x 身份认证方法列表。

```
Switch(config)#aaa authentication dot1x default method1 [method2...]
```

如果采用本地认证方式，则参数 *method* 为 local；如果采用远端认证方式，则参数为 group radius。

② 开启 IEEE 802.1x 功能。

```
Switch(config)#dot1x system-auth-control
```

③ 在相应端口上开启 IEEE 802.1x 功能。

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x pae authenticator
```

其中，第二条命令为在端口上启用 IEEE 802.1x 功能，第三条命令为指定端口角色为身份验证者。

(3) 客户端的配置

为简单起见，在这里使用 Windows XP 系统自带的客户端。在默认情况下，Windows XP 上支持 IEEE 802.1x 的服务 Wired AutoConfig 处于关闭状态，因此首先需要将其开启，如图 6-16 所示。



图 6-16　启动 Wired AutoConfig 服务

启动 Wired AutoConfig 服务后，在“本地连接”的属性对话框中将出现“身份验证”选项卡，在该选项卡中选中“启用 IEEE 802.1x 身份验证”复选框并选择网络身份验证方法为“MD5-质询”(**注意**：客户端的身份验证方法要与设备端配置的用户认证方法相一致，由于在 H3C 网络设备上默认的用户认证方法为 CHAP，因此客户端的身份验证方法必须选择为“MD5-质询”)，如图 6-17 所示。

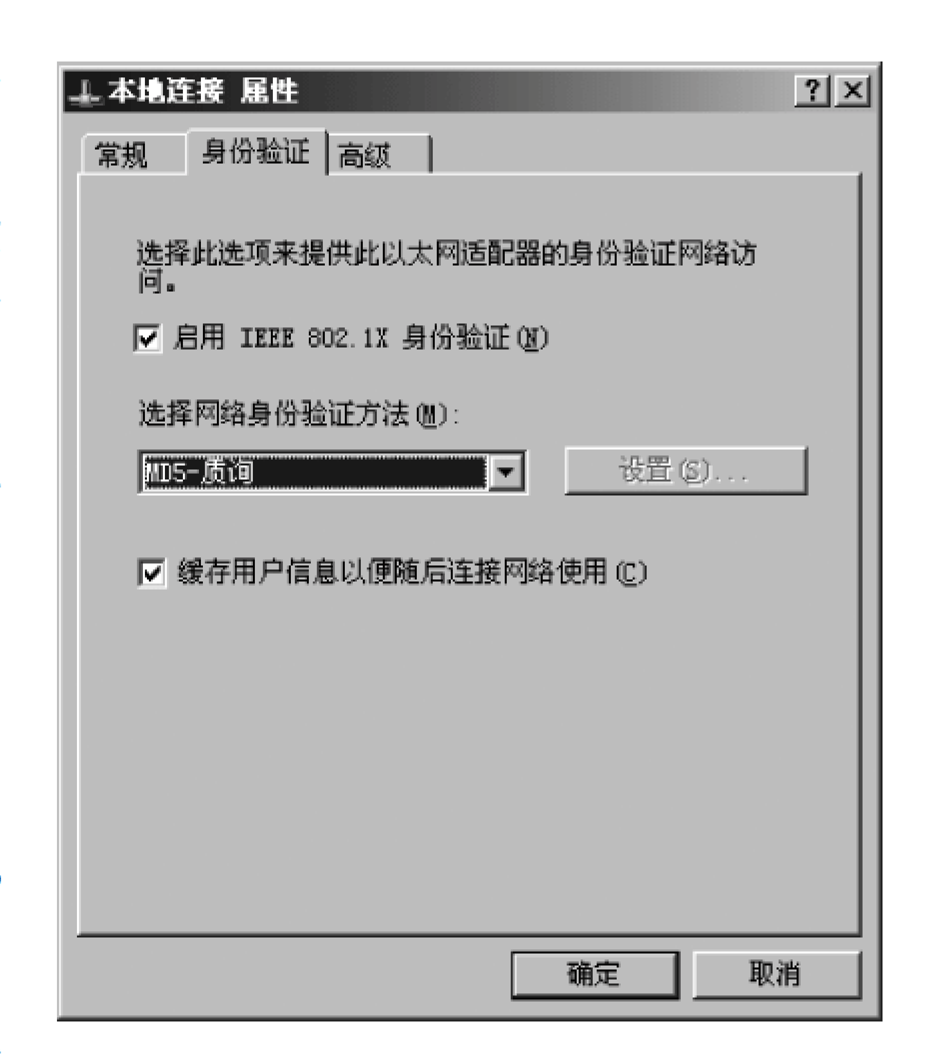


图 6-17　配置“身份验证”选项卡

在配置了身份验证选项后，在系统右下角的任务栏将会出现“需要其他信息以连接到网络”的提示，如图 6-18 所示。

单击网络连接提示，系统弹出“输入凭据”对话框，如图 6-19 所示。



图 6-18 网络连接提示



图 6-19 输入凭据对话框

在“输入凭据”对话框中输入用户名和密码,单击“确定”按钮,Windows XP 就会向设备端发送 EAPOL-Start 报文,开启 IEEE 802.1x 的认证过程。

3. 本地认证配置举例

假设存在如图 6-20 所示的网络,要求配置 IEEE 802.1x 本地认证,使 PC_1 需要通过认证才可以访问外部网络,认证用户名和密码分别为 network 和 123456。

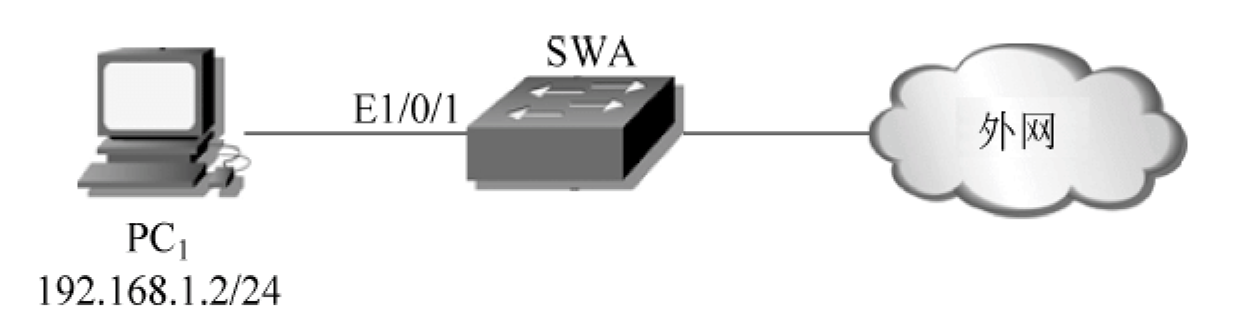


图 6-20 本地认证配置举例

H3C 设备端具体的配置命令如下:

```
[SWA]dot1x
[SWA]undo dot1x handshake enable
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]dot1x
[SWA-Ethernet1/0/1]quit
[SWA]local-user network
[SWA-luser-network]password simple 123456
[SWA-luser-network]service-type lan-access
```

Cisco 设备端具体的配置命令如下:

```
SWA(config)#username network password 123456
SWA(config)#aaa new-model
SWA(config)#aaa authentication dot1x default local
SWA(config)#dot1x system-auth-control
SWA(config)#interface FastEthernet 0/1
SWA(config-if)#switchport mode access
SWA(config-if)#dot1x port-control auto
```

```
SWA(config-if)#dot1x pae authenticator
```

客户端配置参考 6.3.2 小节的内容。

配置完成后，在客户端的“输入凭据”对话框中输入用户名和密码，同时开启 Wireshark 捕获数据报文。从捕获的数据报文中可以看到 IEEE 802.1x 认证的过程，如图 6-21 所示。

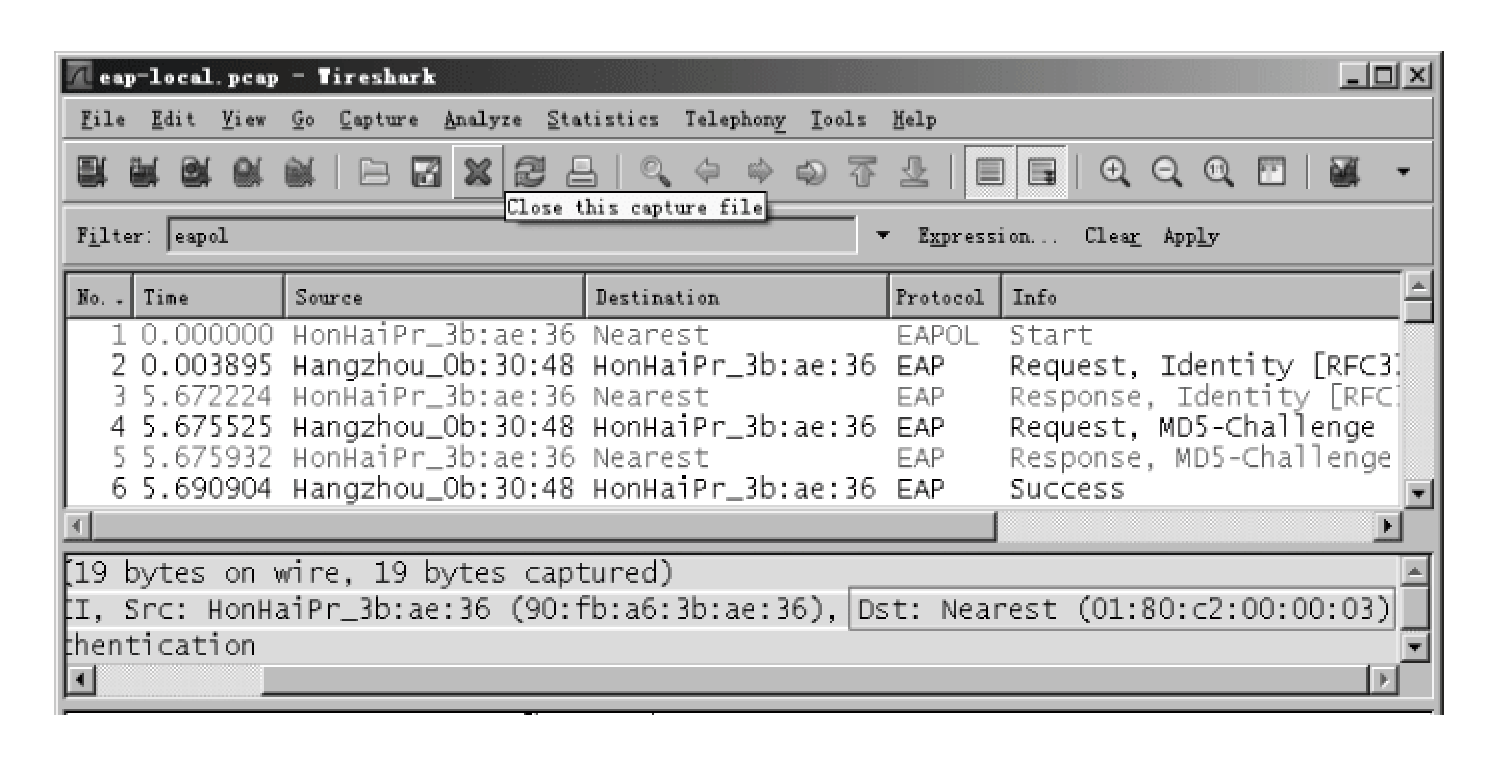


图 6-21　IEEE 802.1x 认证过程

从上图中可以看出，客户端发送给设备端 EAP 报文的目的 MAC 地址均为 01:80:c2:00:00:03，该地址为 IEEE 定义的一个组播 MAC 地址。

认证成功后，PC_1 即可访问外部网络资源。但是客户端每隔 30s 左右就会重新进行一次认证，使用 Wireshark 捕获数据报文会发现设备端每隔 30s 就会向客户端发送一个 EAP-Request/Identity 报文，从而触发了客户端重新进行认证。在设备端的配置中已经关闭了在线用户握手功能，设备端不会向客户端发送握手请求报文，而且握手请求报文的发送时间间隔也不是 30s。那设备端为什么会以 30s 为间隔不断发送 EAP-Request/Identity 报文呢？这就涉及 IEEE 802.1x 的认证触发方式，IEEE 802.1x 的认证触发方式分为两种：

(1) 客户端主动触发方式：客户端主动向设备端发送 EAPOL-Start 报文来触发认证。

(2) 设备端主动触发方式：为兼容不支持主动发起认证的客户端，设备端会每间隔一定的时间主动向客户端发送 EAP-Request/Identity 报文来触发认证。发送时间间隔由传送超时定时器 tx-period 来定义，默认为 30s。

问题已经很明朗，设备端发送的 EAP-Request/Identity 报文实际上是触发认证报文，正是因为有了它的存在，客户端才会不断地重新进行认证。传送超时定时器可以使用命令[H3C]dot1x timer tx-period *tx-period-value* 来进行修改。

将 SWA 上的传送超时定时器修改为最大值 120s，具体的配置命令如下：

```
[SWA]dot1x timer tx-period 120
```

配置完成后，在客户端使用 Wireshark 捕获数据报文，会发现客户端重新进行认证的时间间隔变为了 120s。

Windows XP 自带的客户端无法对 H3C 的私有属性(例如在线用户握手功能)提供支持,如果要支持其私有属性,则需要使用 H3C 专门的 IEEE 802.1x 客户端程序 iNode。

使用版本为 V3.60-E6210 的 iNode,在 PC_1 上安装 iNode,在安装之前一定要将 Windows XP 自带的客户端关闭,关闭的方法为将"身份验证"选项卡中的"启用 IEEE 802.1x 身份验证"选项取消选中,或者直接停止 Wired AutoConfig 服务。

iNode 安装完成后会提示是否重新启动计算机,选择"否,稍后再重新启动计算机"单选按钮即可。此时在桌面上会出现"iNode 智能客户端"的图标,双击该图标,出现 iNode 智能客户端的界面,并会弹出"确认启动新建连接向导"对话框,如图 6-22 所示。

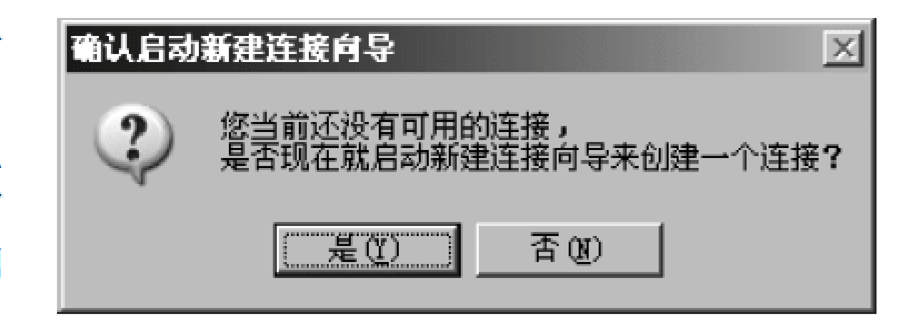


图 6-22 "确认启动新建连接向导"对话框

在图 6-22 中单击"是",进入"新建连接向导"界面,在该界面上单击"下一步"进入"选择认证协议"界面,如图 6-23 所示。

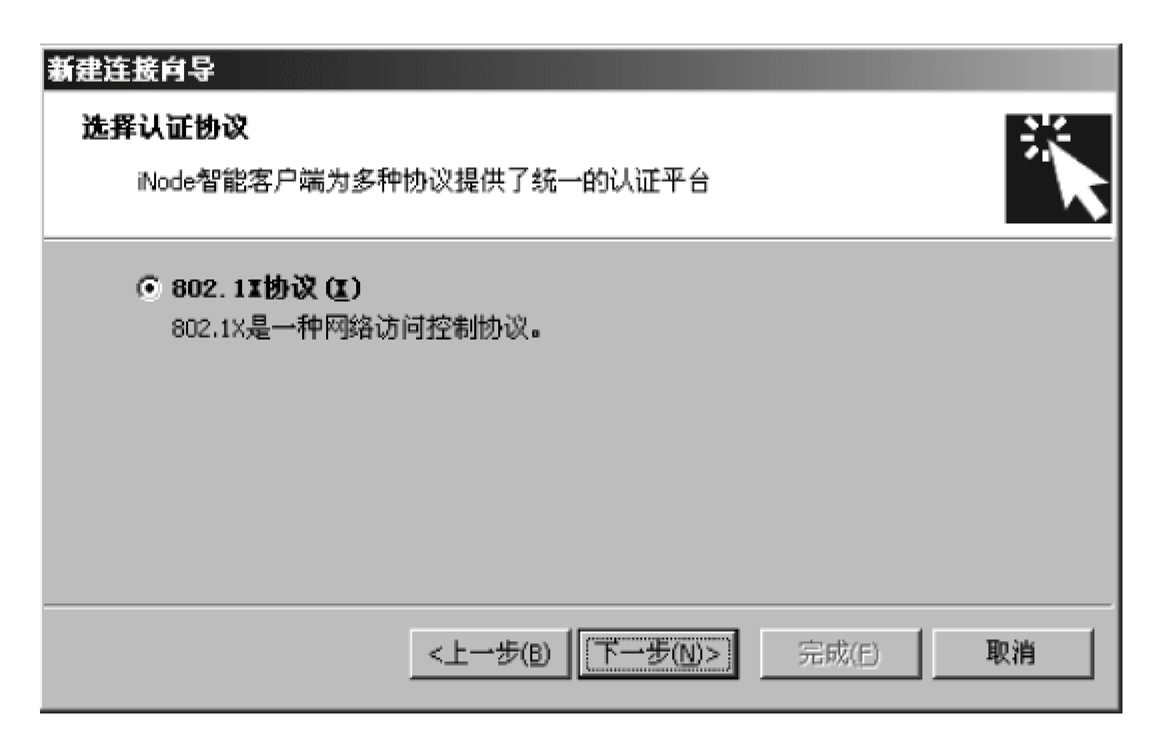


图 6-23 "选择认证协议"界面

在有些版本的 iNode 上,"选择认证协议"界面上除了 802.1x 协议外还有一个 Portal 协议(用于宽带认证上网)供选择,在此选择"802.1x 协议"单选按钮。单击"下一步(N)"进入"选择连接类型"界面,如图 6-24 所示。

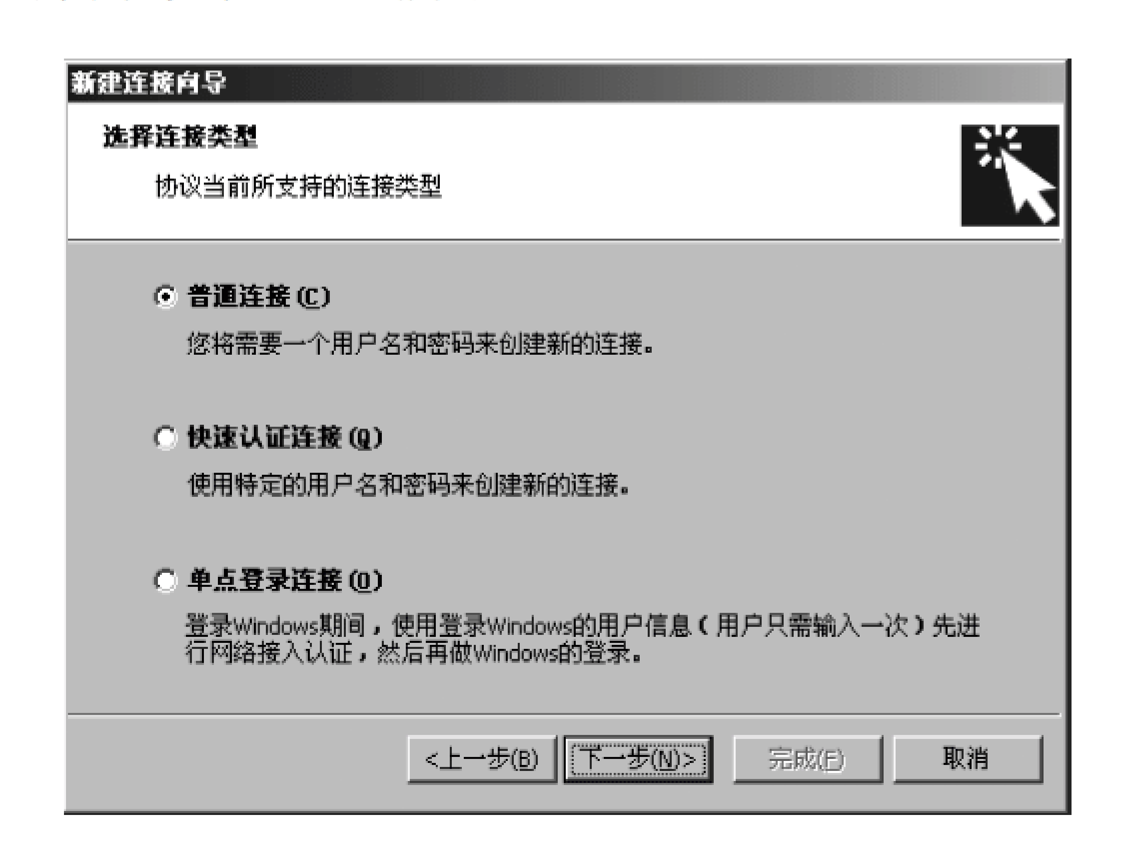


图 6-24 "选择连接类型"界面

在“选择连接类型”界面上选择“普通连接”单选按钮，单击“下一步(N)”进入“账户信息”界面，如图 6-25 所示。

图 6-25　“账户信息”界面

在“账户信息”界面上，输入用户名 network 和密码 123456，单击“下一步(N)”进入“连接属性”界面，如图 6-26 所示。



图 6-26　“连接属性”界面

在“连接属性”界面中选择网卡并进行用户选项等的设置，其中“报文类型”选择单播

报文和多播报文均可,如果选择为单播报文,则客户端发送给设备端的报文除 EAPOL-Start 使用的目的 MAC 地址为 01:80:c2:00:00:03,其他所有报文使用的目的地址均为设备端的 MAC 地址;如果选择为多播报文,则客户端发送给设备端的所有报文使用的目的 MAC 地址均为 01:80:c2:00:00:03。“用户选项”部分除“被动下线时自动重连”外其他的选项均不要选择。



图 6-27 “我的 802.1x 连接”对话框

“连接属性”部分配置完成后,单击“完成”按钮进入“正在完成新建连接向导”界面,在该界面单击“创建”按钮完成 IEEE 802.1x 连接的创建。此时在“iNode 智能客户端”界面上会出现一个“我的 802.1x 连接”图标,右击该图标并选择“连接”,弹出“我的 802.1x 连接”对话框,如图 6-27 所示。

在“我的 802.1x 连接”中单击“连接”按钮,客户端发起 IEEE 802.1x 认证过程,并在“iNode 智能客户端”界面上显示认证信息。如图 6-28 所示。



图 6-28 IEEE 802.1x 认证信息

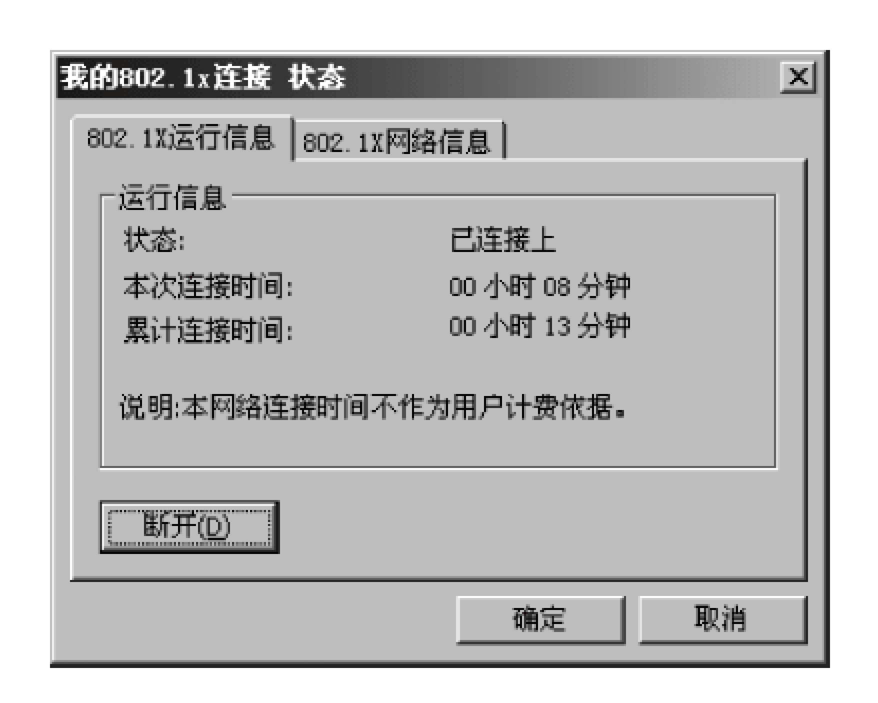


图 6-29 “我的 802.1x 连接 状态”对话框

从图 6-28 上可以看到 IEEE 802.1x 认证成功,此时 PC_1 即可访问外部网络资源。在系统右下角的任务栏将会出现一个“我的 802.1x 连接,通过 802.1x 认证”的图标,双击该图标,将会弹出“我的 802.1x 连接 状态”对话框,显示当前 IEEE 802.1x 的运行信息和网络信息。如图 6-29 所示。

在使用 iNode 作为客户端时,使用 Wireshark 捕获数据报文可以发现对于设备端发送的触发认证报文 EAP-Request/Identity,客户端只是用 EAP-Response/Identity 进行响应,而不会进行重

新认证。

由于 iNode 客户端支持在线用户握手功能，因此可以在设备端开启该功能，具体命令如下：

```
[SWA]dot1x handshake enable
```

配置在线用户握手功能后，使用 Wireshark 捕获数据报文可以看到对于设备端握手请求报文 EAP-Request/Identity，客户端使用握手回应报文 EAP-Response/Identity 进行响应。

无论是在线用户握手还是触发认证，设备端发送的都是 EAP-Request/Identity 报文，而客户端都是以 EAP-Response/Identity 报文进行响应。但是，设备端发送的触发认证报文 EAP-Request/Identity 中的目的 MAC 地址为 01:80:c2:00:00:03；而握手请求报文 EAP-Request/Identity 中的目的 MAC 地址为客户端的 MAC 地址。

注意：如果在某端口上启用了 IEEE 802.1x，则不能配置该端口加入汇聚组；而如果某端口已经加入到了某个汇聚组中，则禁止在该端口上启用 IEEE 802.1x。

6.3.4 IEEE 802.1x 远端认证

在第 6.3.2 小节中提到 IEEE 802.1x 使用 EAP 协议进行认证，在客户端 PAE 和设备端 PAE 之间，EAP 协议通过 EAPOL 的方式直接承载于以太网环境中；而在设备端 PAE 和认证服务器之间则必须使用 RADIUS 协议进行交互，此时 EAP 协议的认证信息就需要使用 RADIUS 协议进行传递。根据 EAP 信息在 RADIUS 报文中承载方式的不同，可以将其分成两种。

(1) EAP 中继方式：采用 EAP 中继方式(EAP Over RADIUS，EAPOR)时，设备端 PAE 将完整的 EAP 报文直接封装在 RADIUS 报文中传递给认证服务器。RADIUS 专门有两个属性来支持 EAP 中继方式，分别是用来封装 EAP 报文的 EAP-Message 属性(属性编码为 79)和保障数据安全的 Message-Authenticator 属性(属性编码为 80)。

(2) EAP 终结方式：采用 EAP 终结方式时，EAP 协议报文在设备端被终结，设备端 PAE 将 EAP 报文中的有用参数信息放置在 RADIUS 报文中的 PAP 或 CHAP 属性参数中传递给认证服务器。

具体采用哪一种认证方式在 H3C 设备上可以使用如下命令进行配置：

```
[H3C]dot1x authentication-method {chap|pap|eap}
```

其中，CHAP 和 PAP 是 EAP 终结方式的两种不同认证方法，而 eap 是 EAP 中继方式。系统默认采用 EAP 终结方式中的 CHAP 认证方法。对于本地认证而言只能采用 EAP 终结方式，即 CHAP 或者 PAP 的认证方法，不能配置为 EAP 中继方式。

1. 远端认证流程

(1) EAP 中继方式认证流程

EAP 中继方式有 4 种不同的认证方法，具体说明如下。

① EAP-MD5：验证客户端的身份，RADIUS 服务器发送 MD5 加密字给客户端，客户端使用该加密字对密码进行加密处理，再传送给 RADIUS 服务器进行认证。

② EAP-TLS：TLS全称是Transport Layer Security，即传输层安全。在EAP-TLS认证方法中，客户端和RADIUS服务器之间检查彼此的安全证书，验证对方的身份，保证通信目的端的正确性，防止网络数据被窃听。

③ EAP-TTLS：TTLS全称是Tunneled Transport Layer Security，即隧道传输层安全。EAP-TTLS是对EAP-TLS的扩展，它使用TLS建立起来的安全隧道传递信息。

④ PEAP：PEAP全称是Protected Extensible Authentication Protocol，即受保护的可扩展认证协议。它首先创建和使用TLS安全通道来进行完整性保护，然后在该通道上进行新的EAP协商，从而完成对客户端的身份验证。

在此以EAP-MD5认证方法为例介绍其认证流程，具体如图6-30所示。

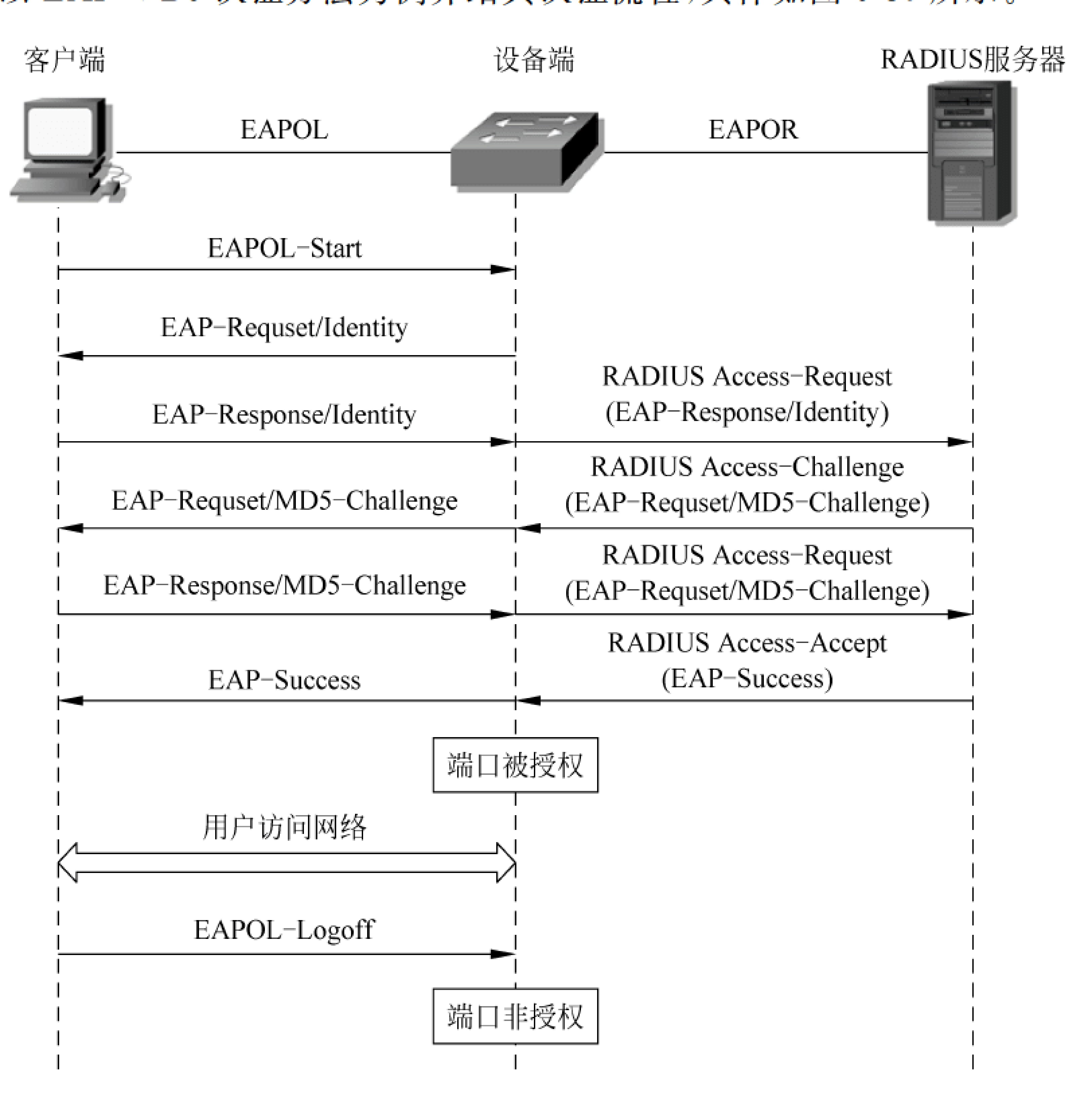


图6-30　EAP中继方式认证流程

① 在用户有访问网络的需求时，打开IEEE 802.1x客户端程序输入用户名和密码，客户端程序向设备端发送EAPOL-Start报文，开始启动一次认证过程。

② 设备端收到来自客户端的EAPOL-Start报文后，向客户端发出EAP-Request/Identity报文，要求客户端发送输入的用户名，来查询客户端的身份。

③ 客户端响应设备端的用户身份查询请求，将用户名信息通过EAP-Response/Identity报文发送给设备端。设备端将从客户端收到的EAP-Response/Identity报文封装到RADIUS Access-Request报文中发送给RADIUS服务器。

④ RADIUS服务器收到设备端转发来的用户名信息后，将其与数据库中的用户名进

行比对，找到该用户名对应的密码，并使用随机生成的一个加密字对密码进行加密处理，同时将随机加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端通过 EAP-Request/MD5-Challenge 报文发送给客户端。

⑤ 客户端收到设备端发来的 EAP-Request/MD5-Challenge 报文后，使用其中的随机加密字对密码进行加密处理，并将加密后的密码通过 EAP-Response/MD5-Challenge 报文发送给设备端。设备端将从客户端收到的 EAP-Response/MD5-Challenge 报文封装到 RADIUS Access-Request 报文中发送给 RADIUS 服务器。

⑥ RADIUS 服务器收到设备端转发来的密码信息后，将其与自己计算出的加密密码进行比对，若两者相同，则认为用户合法，向设备端发送 RADIUS Access-Accept 报文。设备端接收到该报文后，向客户端发送 EAP-Success 报文，通知客户端 IEEE 802.1x 认证通过，同时将受控端口的状态改为授权状态，允许用户通过该端口访问网络。

⑦ 用户下线时，客户端向设备端发送 EAPOL-Logoff 报文，设备端将受控端口的状态由授权状态改为非授权状态，不再允许用户通过该端口访问网络。

注意：由于在使用 EAP 中继方式进行认证时，设备端只是将 EAP 报文封装到 RADIUS 报文中，或从 RADIUS 报文中解封装出 EAP 报文，而不会对 EAP 报文的内容做任何改动，因此具体是使用 EAP-MD5、EAP-TLS、EAP-TTLS 和 PEAP 这 4 种认证方法中的哪一种由客户端和 RADIUS 服务器共同决定，与设备端无关。在设备端上只需要通过[H3C]dot1x authentication-method eap 命令启动 EAP 中继方式即可。

（2）EAP 终结方式认证流程

在此以 CHAP 认证方法为例介绍 EAP 终结方式的认证流程，具体如图 6-31 所示。

① 在用户有访问网络的需求时，打开 IEEE 802.1x 客户端程序输入用户名和密码，客户端程序向设备端发送 EAPOL-Start 报文，开始启动一次认证过程。

② 设备端收到来自客户端的 EAPOL-Start 报文后，向客户端发出 EAP-Request/Identity 报文，要求客户端发送输入的用户名，来查询客户端的身份。

③ 客户端响应设备端的用户身份查询请求，将用户名信息通过 EAP-Response/Identity 报文发送给设备端。

④ 设备端收到客户端发来的 EAP-Response/Identity 报文后，暂存其中的用户名信息，随机生成一个加密字并将其通过 EAP-Request/MD5-Challenge 报文发送给客户端。

⑤ 客户端收到设备端发来的 EAP-Request/MD5-Challenge 报文后，使用其中的随机加密字对密码进行加密处理，并将加密后的密码通过 EAP-Response/MD5-Challenge 报文发送给设备端。

⑥ 设备端从接收到的 EAP-Response/MD5-Challenge 报文中获得客户端使用随机加密字加密的密码，然后将该密码和暂存的用户名以及随机加密字通过 RADIUS Access-Request 报文发送给 RADIUS 服务器。

⑦ RADIUS 服务器从收到的 RADIUS Access-Request 报文中获取用户名、加密密码和加密字信息，并将获取的用户名与其数据库中的用户名进行比对，找到该用户名对应的密码，然后使用获取的随机加密字对密码进行加密处理，并将加密处理结果与获取的加密密码进行比对，若两者相同，则认为用户合法，向设备端发送 RADIUS Access-Accept

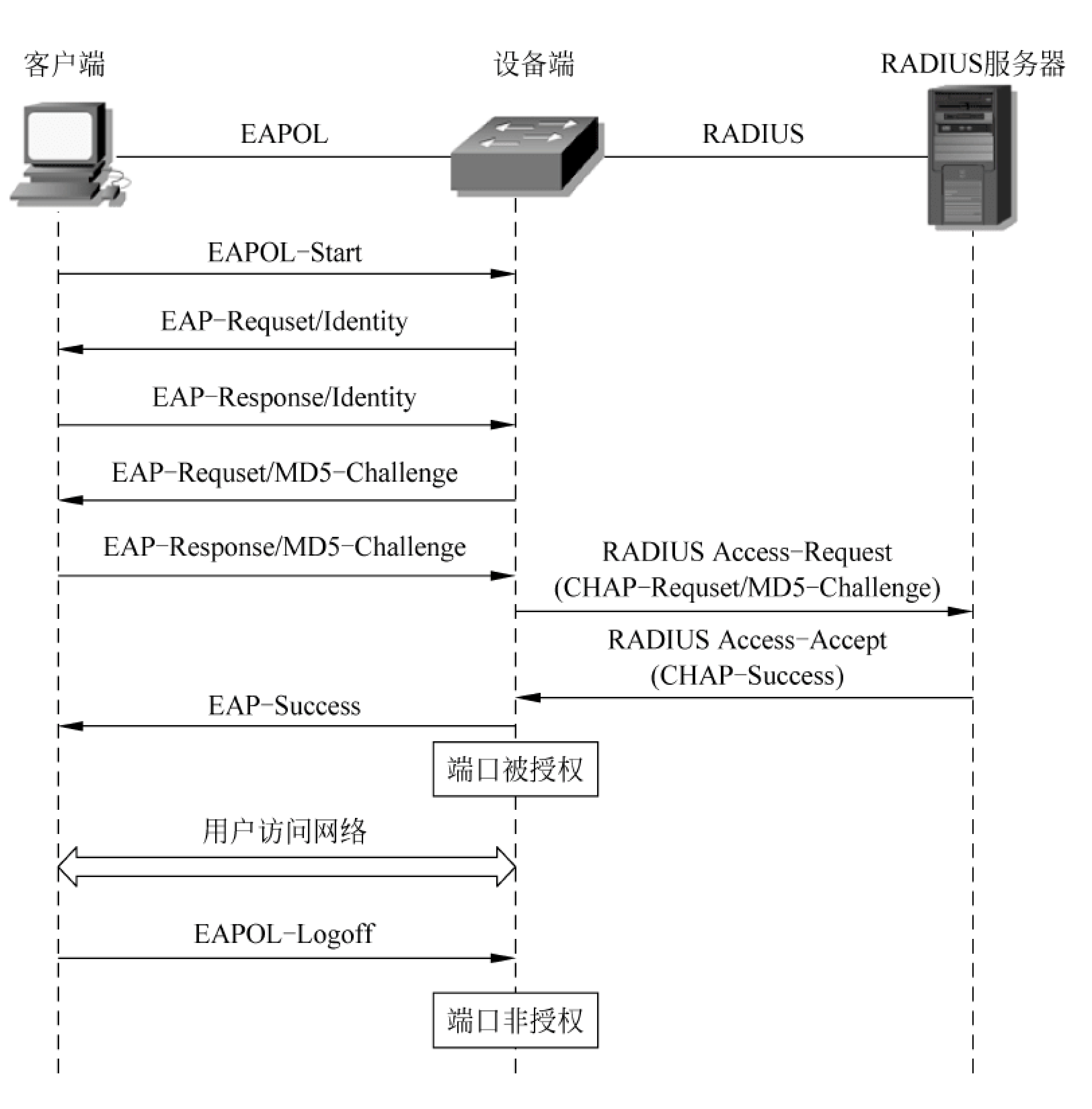


图 6-31 EAP 终结方式认证流程

报文。设备端接收到该报文后，向客户端发送 EAP-Success 报文，通知客户端 IEEE 802.1x 认证通过，同时将受控端口的状态改为授权状态，允许用户通过该端口访问网络。

⑧ 用户下线时，客户端向设备端发送 EAPOL-Logoff 报文，设备端将受控端口的状态由授权状态改为非授权状态，不再允许用户通过该端口访问网络。

2. 远端认证配置举例

远端认证涉及的配置命令在第 6.2.2 小节和第 6.3.3 小节中已做过详细讲解，在此不再进行介绍。

假设存在如图 6-32 所示的网络，交换机型号为 H3C E126A，要求配置 IEEE 802.1x 远端认证，认证方法使用 EAP 终结方式中的 CHAP 认证方法，PC_1 需要通过认证才可以访问外部网络，认证用户名和密码分别为 network 和 123456；设备端配置的 AAA 域名为 study；设备端与 RADIUS 服务器之间的共享密钥为 test。

H3C 设备端上具体的配置命令如下：

```
[SWA]dot1x
[SWA]undo dot1x handshake enable
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]dot1x
[SWA-Ethernet1/0/1]quit
```

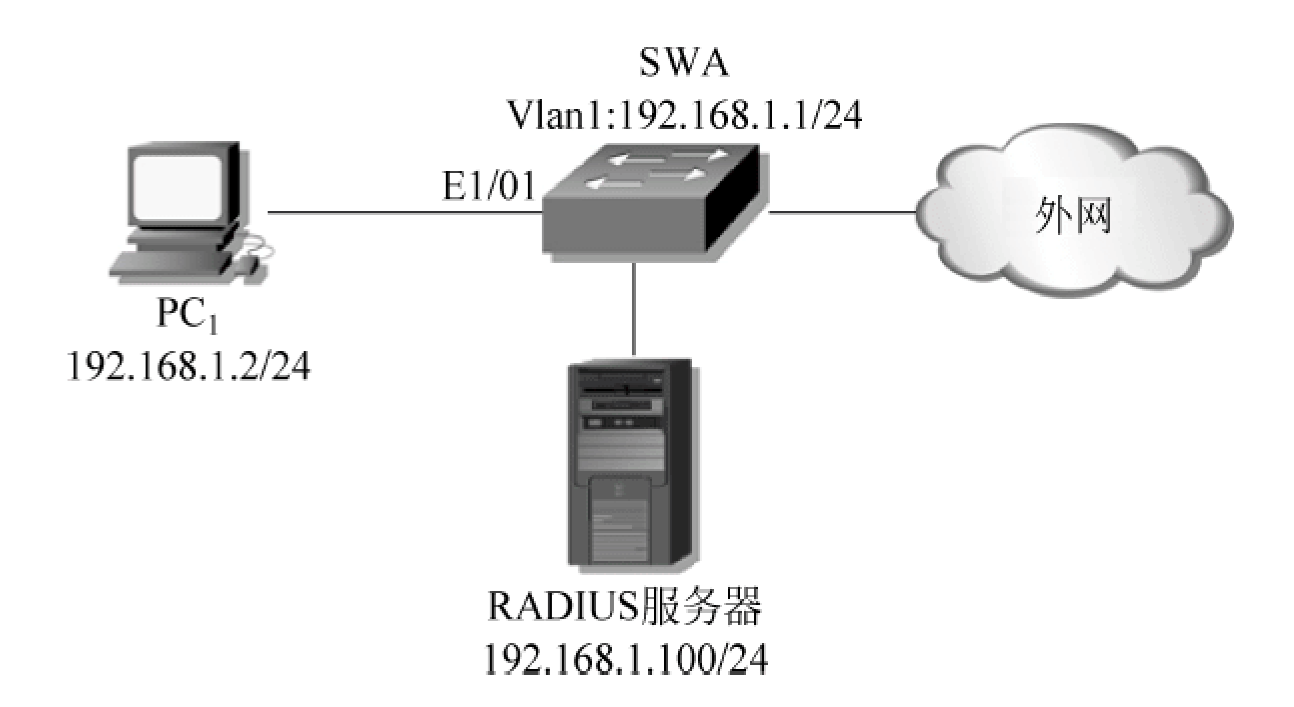


图 6-32　远端认证配置举例

```
[SWA]radius scheme LanAcc
[SWA-radius-LanAcc]primary authentication 192.168.1.100 1812
[SWA-radius-LanAcc]primary accounting 192.168.1.100 1813
[SWA-radius-LanAcc]nas-ip 192.168.1.1
[SWA-radius-LanAcc]key authentication test
[SWA-radius-LanAcc]key accounting test
[SWA-radius-LanAcc]user-name-format with-domain
[SWA-radius-LanAcc]server-type standard
[SWA-radius-LanAcc]quit
[SWA]domain study
[SWA-isp-study]authentication radius-scheme LanAcc
[SWA-isp-study]accounting radius-scheme LanAcc
[SWA-isp-study]accounting optional
[SWA-isp-study]quit
[SWA]domain default enable study
```

Cisco 设备端上具体的配置命令如下：

```
SWA(config)#aaa new-model
SWA(config)#radius-server host 192.168.1.100 auth-port 1812 acct-port 1813
SWA(config)#radius-server key test
SWA(config)#aaa authentication dot1x default group radius
SWA(config)#dot1x system-auth-control
SWA(config)#interface FastEthernet 0/1
SWA(config-if)#switchport mode access
SWA(config-if)#dot1x port-control auto
SWA(config-if)#dot1x pae authenticator
```

RADIUS 服务器的配置如下：
（配置文件 clients.conf 的末尾添加如下信息。）

```
client 192.168.1.1/24 {
        secret        = test
        shortname     = SWA
}
```

配置文件 users.conf 的开始位置添加如下信息:

network@study User-Password == "123456"

注意: 如果交换机 SWA 为 Cisco 设备,则配置文件 users.conf 中的用户名为 network。

配置完成后,重新启动 FreeRADIUS 服务。

客户端使用 Windows XP 自带的客户端软件或者使用 H3C 的 iNode 客户端软件均可,配置略。

配置完成后,在客户端软件中输入用户名和密码,启动 IEEE 802.1x 认证过程,同时在 PC_1 和 RADIUS 服务器上开启 Wireshark 捕获数据报文。

对比 PC_1 上捕获的 EAPOL 报文和 RADIUS 服务器上捕获的 RADIUS 报文,会发现如下信息:

(1) 在 PC_1 上捕获的 EAP-Request/MD5-Challenge 报文中 Value 属性的值和在 RADIUS 服务器上捕获的 RADIUS Access-Request 报文中 CHAP-Challenge 属性的值相同,该值为设备端生成的随机加密字。

(2) 在 PC_1 上捕获的 EAP-Response/MD5-Challenge 报文中的 Value 属性的值和在 RADIUS 服务器上捕获的 RADIUS Access-Request 报文中 CHAP-Password 属性的值相同,该值为使用随机加密字加密后的用户密码。

具体如图 6-33～6-35 所示,这也验证了 EAP 终结方式的认证流程。

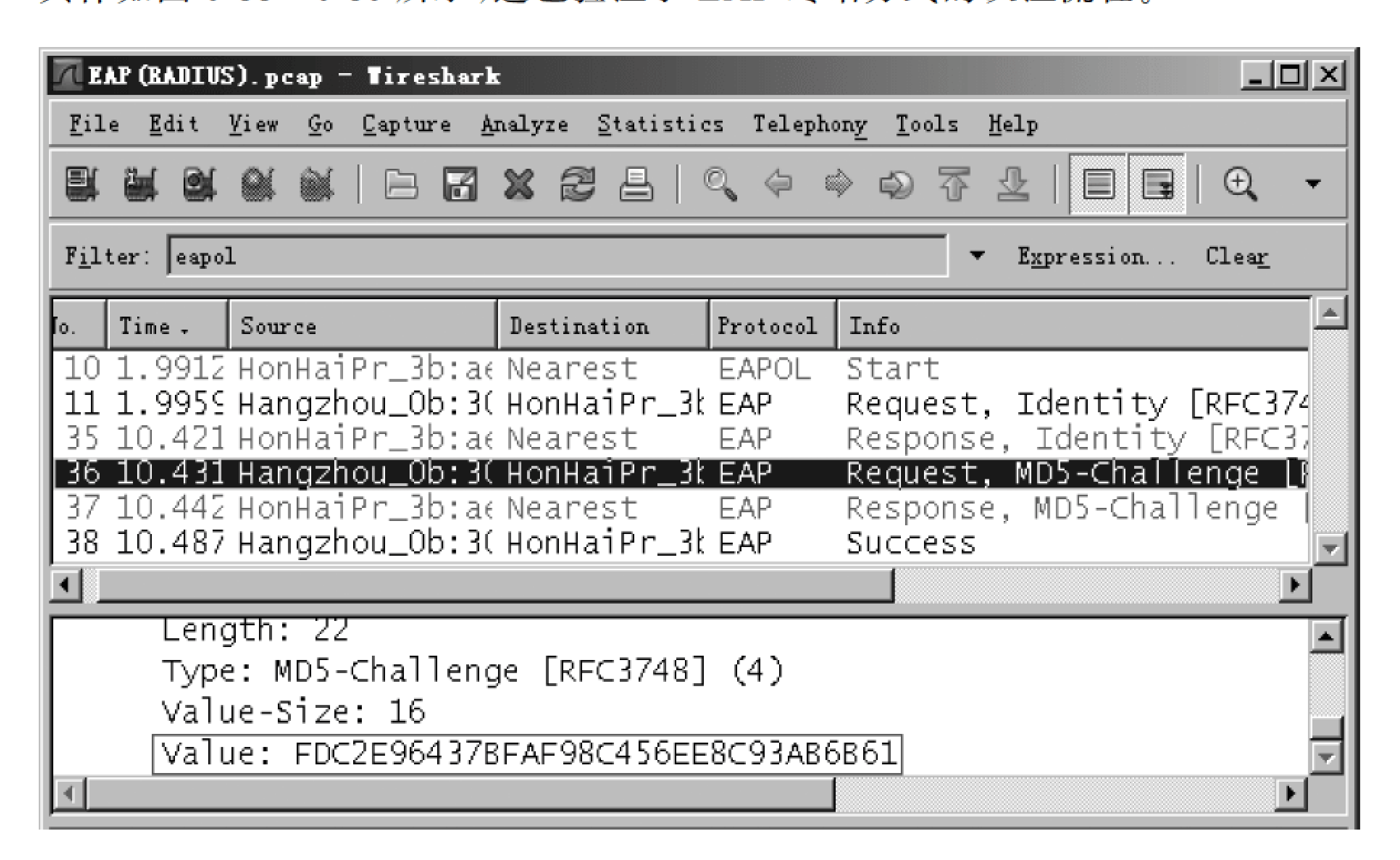


图 6-33 EAP-Request/MD5-Challenge 中 Value 的值①

认证成功后,PC_1 即可访问外部网络资源。

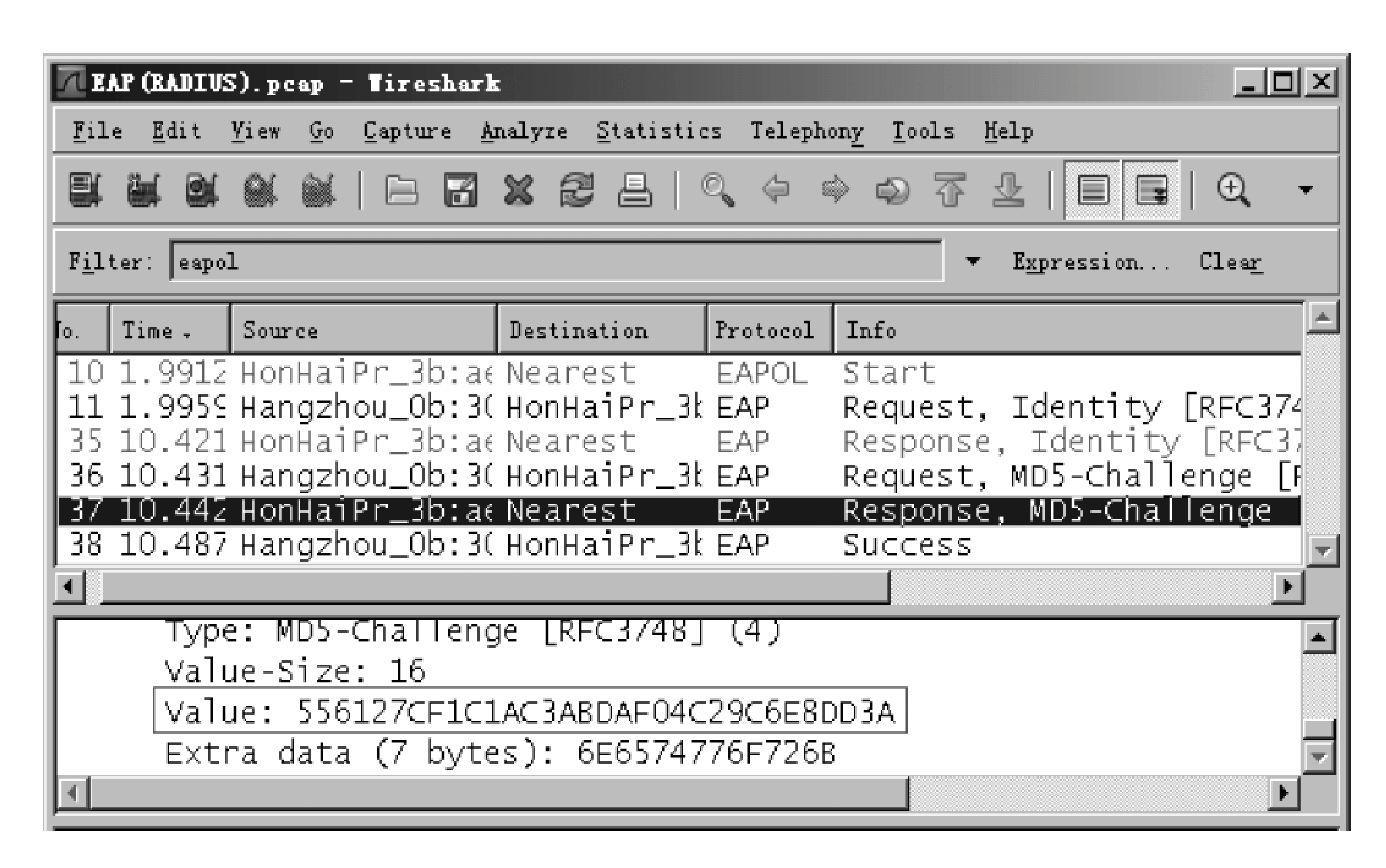


图 6-34　EAP-Response/MD5-Challenge 中 Value 的值②

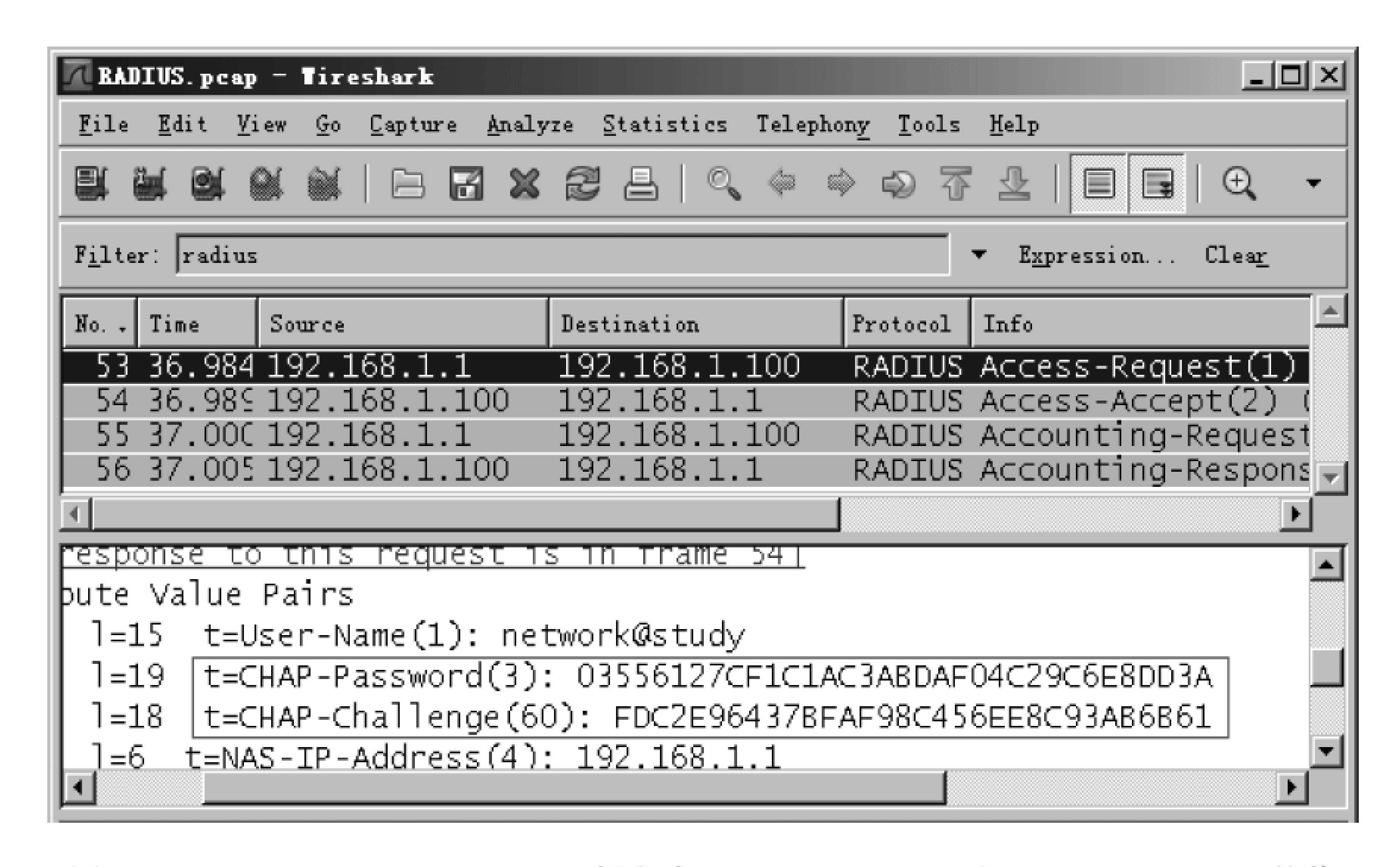


图 6-35　RADIUS Access-Request 报文中 CHAP-Challenge 和 CHAP-Password 的值

6.4　端口安全技术

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，它通过定义各种端口安全模式，让网络设备端口学习到该端口下合法的终端 MAC 地址，然后通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备对网络的访问；通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。端口安全是对已有的 IEEE 802.1x 认证和 MAC 地址认证的扩充。

MAC地址认证是一种基于端口和MAC地址对用户的网络访问权限进行控制的认证方法,与IEEE 802.1x类似,同样也分为本地认证和远端RADIUS服务器认证两种方式。MAC地址认证一般以MAC地址作为认证的用户名。关于MAC地址认证的知识在本书中不再进行介绍,感兴趣的读者可以自行查阅相关资料。

6.4.1 端口安全基础

1. 端口安全的特性

端口安全包括3个特性,具体说明如下。

(1) NTK特性:NTK(Need To Know)特性通过检测从端口发出数据帧的目的MAC地址,保证数据帧只能被发送到已经通过认证的设备上,从而防止非法设备窃听网络数据。

(2) Intrusion Protection特性:即入侵检测特性,该特性检测端口收到数据帧的源MAC地址,若某端口收到了源MAC地址为非法MAC的数据帧,则对该端口采取相应的安全策略,包括暂时断开连接、永久断开连接或者过滤源MAC地址为该非法MAC的数据帧,以确保端口的安全性。

(3) Trap特性:该特性是在端口有特定的数据帧(如非法入侵、IEEE 802.1x认证失败、用户上下线等产生的数据帧)传送时,网络设备将发送Trap消息,便于网管员对其进行监控。

2. 端口安全的模式

不同型号的网络设备支持的端口安全模式种类会有所区别,但一般都会有十几种模式。由于大部分模式均与IEEE 802.1x认证和MAC地址认证有关,相对比较复杂,因此不对其进行介绍。在这里只对最简单并独立于IEEE 802.1x认证和MAC地址认证的3种端口安全模式进行介绍。

(1) noRestrictions模式:此模式为端口的默认模式,在此模式下端口处于无限制状态。

(2) autolearn模式:在此模式下,端口通过手工配置或自动学习到的安全MAC地址被保存在安全MAC地址表中。当端口下的安全MAC地址数达到了端口配置的最大安全MAC地址数后,端口模式会自动转变为secure模式,并停止添加新的安全MAC地址。此后,只有源MAC地址为安全MAC地址的数据帧才能通过该端口。

(3) secure模式:在此模式下,禁止端口学习MAC地址。只有源MAC地址为安全MAC地址的数据帧才能通过该端口。

6.4.2 端口安全的配置

在此以H3C E126A交换机为例,介绍端口安全配置涉及的命令。

(1) 启动端口安全功能。

```
[H3C]port-security enable
```

默认情况下,端口安全功能处于关闭状态。需要注意的是,IEEE 802.1x/MAC地址认证功能与端口安全功能不能同时开启,否则系统会提示错误。例如,在开启了IEEE

802.1x 认证后，如果再配置端口安全功能，系统提示错误如下：

```
[H3C]port-security enable
Port-security can not be configured for dot1x is enabled.
```

同样，在启动了端口安全的功能后，IEEE 802.1x 认证和 MAC 地址认证均不能再进行手动配置，而只能随着端口安全模式的改变由系统进行配置。

（2）配置端口允许的最大安全 MAC 地址数。

```
[H3C-Ethernet1/0/1]port-security max-mac-count count-value
```

通过配置端口允许的最大安全 MAC 地址数，可以控制某端口接入网络的最大用户数量。一旦某端口上的安全 MAC 达到了 *count-vlaue* 的值，则该端口将不再学习任何安全 MAC 地址。

（3）配置端口安全模式。

```
[H3C-Ethernet1/0/1]port-security port-mode autolearn
```

由于只对最简单的三种端口安全模式进行了介绍，其中 noRestrictions 模式为端口默认模式，secure 模式下不进行安全 MAC 地址的学习，所以需要将端口安全模式配置为 autolearn。需要注意的是，在配置端口为 autolearn 模式时，必须已经配置了端口允许的最大安全 MAC 地址数，否则系统会提示错误，具体如下：

```
[H3C-Ethernet1/0/1]port-security port-mode autolearn
Cannot enable autolearn when max mac-address count is not set.
```

另外，如果某端口上配置了端口安全模式，则不能配置该端口加入汇聚组；而如果某端口已经加入到了某个汇聚组中，则禁止在该端口上配置端口安全模式。

（4）配置安全 MAC 地址。

```
[H3C-Ethernet1/0/1]mac-address security mac-address vlan vlan-id
```

通过手动配置的安全 MAC 地址与端口自动学习到的安全 MAC 地址性质完全相同，无论是手动配置还是自动学习的安全 MAC 地址都不会被老化，并且会被写入到配置文件中，在保存配置文件后，即使重启设备，安全 MAC 地址也不会丢失。

在同一个 VLAN 中，一个安全 MAC 地址只能被添加到一个端口上，因此可以实现同一 VLAN 内 MAC 地址与端口的绑定。

在 H3C S3610 交换机上配置安全 MAC 地址的命令为：

```
[H3C-Ethernet1/0/1]port-security mac-address security mac-address vlan vlan-id
```

（5）配置端口安全的特性。

① 配置 NTK 特性。

```
[H3C-Ethernet1/0/1]port-security ntk-mode {ntkonly|ntk-withbroadcasts|ntk-withmulticasts}
```

其中，ntkonly 是指仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过；ntk-withbroadcasts 是指允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文

或目的MAC地址为广播地址的报文通过；ntk-withmulticasts是指允许目的MAC地址为已通过认证的MAC地址的单播报文以及目的MAC地址为广播地址或组播地址的报文通过。

默认情况下，端口上没有配置NTK特性。

② 配置Intrusion Protection特性。

```
[H3C-Ethernet1/0/1]port-security intrusion-mode {blockmac|disableport|disableport-temporarily}
```

Intrusion Protection特性用来配置当网络设备检测到一个非法报文试图通过端口访问网络时，网络设备所采取的安全措施。其中，blockmac表示将源MAC地址为非法MAC的非法报文阻塞，即丢弃掉；disableport表示将收到非法报文的端口永久关闭；disableport-temporarily表示将收到非法报文的端口暂时关闭一段时间，默认为20s，该时间可以通过下面的命令进行调整：

```
[H3C]port-security timer disableport time-value
```

默认情况下，端口上没有配置Intrusion Protection特性。

③ 配置Trap特性。

```
[H3C]port-security trap
{addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion | ralmlogfailure | ralmlogoff |
ralmlogon}
```

注意：与NTK特性和Intrusion Protection特性在具体的端口视图下配置不同，Trap特性在系统视图下进行配置。

具体的参数解释如下。

addresslearned：端口学习到新MAC地址时发出报警信息；

dot1xlogfailure/dot1xlogoff/dot1xlogon：IEEE 802.1x用户认证失败/下线/认证成功时发出报警信息；

ralmlogfailure/ralmlogoff/ralmlogon：MAC地址认证用户认证失败/下线/认证成功时发出报警信息；

intrusion：发现非法报文时发出报警信息。

Cisco设备在配置端口安全之前，首先需要保证相应的端口模式为access。

配置涉及的命令如下。

(1) 在端口上启用端口安全特性。

```
Switch(config-if)#switchport port-security
```

(2) 配置端口允许的最大安全MAC地址数。

```
Switch(config-if)#switchport port-security maximum number
```

(3) 配置安全MAC地址。

```
Switch(config-if)#switchport port-security mac-address mac-address
```

（4）配置端口启用动态学习 MAC 地址。

```
Switch(config-if)#switchport port-security mac-address sticky
```

（5）配置端口的安全违规行为模式。

```
Switch(config-if)#switchport port-security violation {protect|restrict|shutdown}
```

该命令的作用实际上相当于 H3C 设备上配置的 Intrusion Protection 特性。其中，参数 protect 是指阻塞源 MAC 地址为非法 MAC 的非法报文，但不发送报警信息；restrict 是指阻塞非法报文，同时发送 syslog 报警信息；shutdown 是指关闭接口。默认安全违规行为模式为 shutdown。

（6）配置端口的关闭时间。

```
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval seconds
```

当端口的安全违规行为模式为 shutdown 时，可以配置端口的关闭时间。第一条命令为打开 errdisable 的计时器，第二条命令为设置计时器的时间间隔，默认为 300s。

假设存在如图 6-36 所示的网络，要求在交换机 SWA 上启用端口安全功能，在端口 Ethernet1/0/1 上最多允许两个用户接入，配置端口的安全模式为 autolearn，配置 Intrusion Protection 特性为暂时关闭端口，关闭时间为 60s。

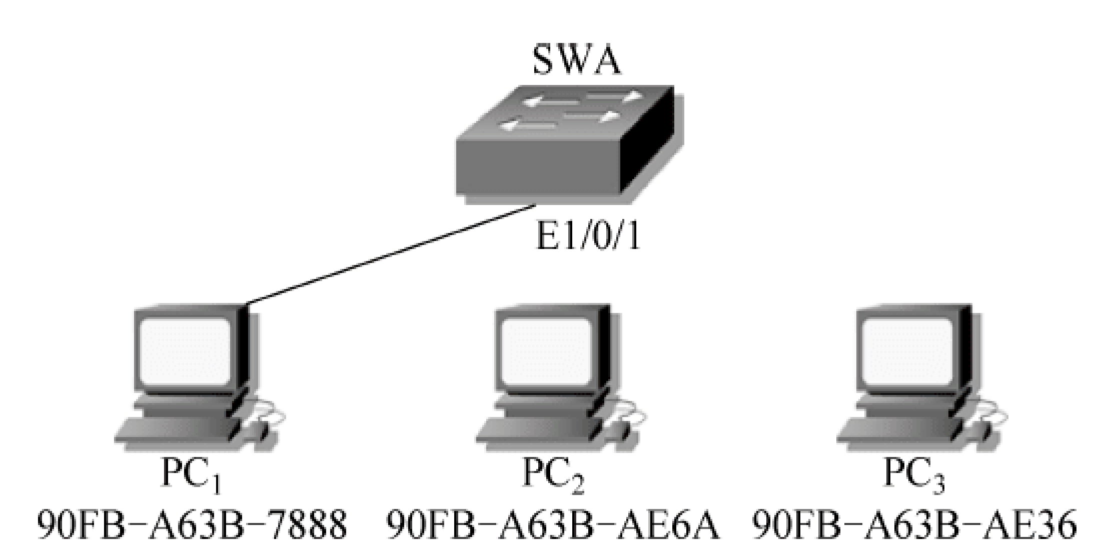


图 6-36　端口安全配置举例

H3C 设备具体的配置命令如下：

```
[SWA]port-security enable
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port-security max-mac-count 2
[SWA-Ethernet1/0/1]port-security port-mode autolearn
[SWA-Ethernet1/0/1]port-security intrusion-mode disableport-temporarily
[SWA-Ethernet1/0/1]quit
[SWA]port-security timer disableport 60
```

Cisco 设备具体的配置命令如下：

```
SWA(config)#interface FastEthernet 0/1
SWA(config-if)#switchport mode access
SWA(config-if)#switchport port-security
SWA(config-if)#switchport port-security maximum 2
```

```
SWA(config-if)#switchport port-security mac-address sticky
SWA(config-if)#switchport port-security violation shutdown
SWA(config-if)#exit
SWA(config)#errdisable recovery cause psecure-violation
SWA(config)#errdisable recovery interval 60
```

配置完成后,在 H3C 设备上使用 display port-security 命令查看端口安全配置信息如下:

```
[SWA]display port-security interface Ethernet 1/0/1
Ethernet1/0/1 is link-up
   Port mode is AutoLearn
   NeedtoKnow mode is disabled
   Intrusion mode is disableportTemporarily
   Max mac-address num is 2
   Stored mac-address num is 1
   Authorization is permit
```

从显示的结果可以看出,端口 Ethernet1/0/1 的模式为 autolearn,Intrusion 特性为 disableportTemporarily,允许的最大安全 MAC 地址数为 2,当前已经存储的安全 MAC 地址数为 1。Authorization is permit 指的是端口应用 RADIUS 服务器下发的授权信息,在这里不需要关注。

在 Cisco 设备上使用 show port-security 命令查看端口安全配置信息如下:

```
SWA#show port-security interface FastEthernet 0/1
Port Security                  : Enabled
Port Status                    : Secure-up
Violation Mode                 : Shutdown
Aging Time                     : 0 mins
Aging Type                     : Absolute
SecureStatic Address Aging     : Disabled
Maximum MAC Addresses          : 2
Total MAC Addresses            : 1
Configured MAC Addresses       : 0
Sticky MAC Addresses           : 1
Last Source Address:Vlan       : 90fb.a63b.7888:1
Security Violation Count       : 0
```

在 H3C 设备上使用 display mac-address security 命令(在 H3C S3610 交换机上命令为 display port-security mac-address security)查看交换机学习到的安全 MAC 地址的信息如下:

```
[SWA]display mac-address security
MAC ADDR        VLAN ID    STATE        PORT INDEX         AGING TIME(s)
90fb-a63b-7888  1          Security     Ethernet1/0/1       NOAGED

  ---  1 mac address(es) found  ---
```

从显示的结果可以看出,在端口 Ethernet1/0/1 上学习到一个安全 MAC 地址 90fb-a63b-7888,即 PC_1 的 MAC 地址。

在 Cisco 设备上使用 show port-security address 命令查看交换机学习到的安全 MAC 地址信息如下：

```
SWA#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address        Type             Ports    Remaining Age (mins)
------  ------------------ ----             -----    -------------
   1    90fb.a63b.7888     SecureSticky     Fa0/1          -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port)  : 8192
```

将 PC_1 从交换机 SWA 上断开，将 PC_2 连接到交换机 SWA 的端口 Ethernet1/0/1 上，然后在 H3C 设备上使用 display port-security 命令查看端口安全配置信息如下：

```
[SWA]display port-security interface Ethernet 1/0/1
Ethernet1/0/1 is link-up
    Port mode is Secure
    NeedtoKnow mode is disabled
    Intrusion mode is disableportTemporarily
    Max mac-address num is 2
    Stored mac-address num is 2
    Authorization is permit
```

从显示的结果可以看出，此时存储的安全 MAC 地址数达到了允许的最大安全 MAC 地址数，而端口的模式自动转变为了 secure。

在 Cisco 设备上使用 show port-security 命令查看端口安全配置信息如下：

```
SWA#show port-security interface FastEthernet 0/1
Port Security                 : Enabled
Port Status                   : Secure-up
Violation Mode                : Shutdown
Aging Time                    : 0 mins
Aging Type                    : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 2
Total MAC Addresses           : 2
Configured MAC Addresses      : 0
Sticky MAC Addresses          : 2
Last Source Address:Vlan      : 90fb.a63b.ae6a:1
Security Violation Count      : 0
```

在 H3C 设备上使用 display mac-address security 命令查看交换机学习到的安全 MAC 地址信息如下：

```
[SWA]display mac-address security
MAC ADDR         VLAN ID    STATE       PORT INDEX          AGING TIME(s)
90fb-a63b-7888   1          Security    Ethernet1/0/1        NOAGED
```

```
90fb-a63b-ae6a    1         Security      Ethernet1/0/1         NOAGED

  ---  2 mac address(es) found  ---
```

从显示的结果可以看出,在端口 Ethernet1/0/1 上又学习到了一个安全 MAC 地址 90fb-a63b-ae6a,即 PC_2 的 MAC 地址。

在 Cisco 设备上使用 show port-security address 命令查看交换机学习到的安全 MAC 地址信息如下:

```
SWA#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------
Vlan     Mac Address        Type            Ports    Remaining Age (mins)
------   ----------------   ----            -----    -------------
   1     90fb.a63b.7888     SecureSticky    Fa0/1    -----
   1     90fb.a63b.ae6a     SecureSticky    Fa0/1    -----
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)       : 1
Max Addresses limit in System (excluding one mac per port)  : 8192
```

将 PC_2 从交换机 SWA 上断开,将 PC_3 连接到交换机 SWA 的端口 Ethernet1/0/1 上,此时在超级终端上可以看到"Ethernet1/0/1 is DOWN"的信息。在 H3C 设备上使用 display port-security 命令查看端口安全配置信息如下:

```
[SWA]display port-security interface Ethernet 1/0/1
Ethernet1/0/1 is link-down
    Port mode is Secure
    NeedtoKnow mode is disabled
    Intrusion mode is disableportTemporarily
    Max mac-address num is 2
    Stored mac-address num is 2
    Authorization is permit
```

从显示的结果可以看出,端口 Ethernet1/0/1 的状态为 link-down。

在 Cisco 设备上使用 show port-security 命令查看端口安全配置信息如下:

```
SWA#show port-security interface fastEthernet 0/1
Port Security                : Enabled
Port Status                  : Secure-shutdown
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 2
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 2
Last Source Address:Vlan     : 90fb.a63b.7888:1
Security Violation Count     : 1
```

将 PC_3 从交换机 SWA 上断开，将 PC_1 或者 PC_2 重新连接到交换机 SWA 的端口 Ethernet1/0/1 上，等待 60s，会发现端口 Ethernet1/0/1 重新回到 UP 状态。

6.5 端口绑定技术

端口绑定技术通过将用户的 IP 地址和 MAC 地址绑定到指定的交换机端口上，使交换机只对从相应端口收到的指定 IP 地址和指定 MAC 地址的数据报文进行转发，从而实现对端口转发的报文进行过滤控制，增强端口的安全性，实现 IP 源防护（IP Source Guard，IPSG）功能。

端口绑定是针对端口的，在一个端口配置了端口绑定后，只是该端口被限制了，而其他端口不受该绑定的影响。

在不同型号的 H3C 交换机上端口绑定的配置也有所不同，在这里以交换机 H3C S3610 和 H3C E126A 为例介绍端口绑定的配置和应用。

6.5.1 H3C S3610 上端口绑定的配置

H3C S3610 上端口绑定的配置命令如下：

[H3C-Ethernet1/0/1] user-bind {ip-address *ip-address* | mac-address *mac-address* | ip-address *ip-address* mac-address *mac-address*} [vlan vlan-id]

在 H3C S3610 交换机上支持 IP、MAC、IP+MAC、IP+VLAN、MAC+VLAN、IP+MAC+VLAN 等 6 种绑定表项的组合，因此它既支持 IP+MAC 的绑定，也支持单独只绑定 IP 地址或单独只绑定 MAC 地址。

假设存在如图 6-37 所示的网络，要求在交换机 SWA 上配置端口绑定，其中将 PC_1 的 IP 地址绑定到端口 Ethernet1/0/1 上、将 PC_2 的 MAC 地址绑定到端口 Ethernet1/0/2 上，将 PC_3 的 IP 地址和 MAC 地址绑定到端口 Ethernet1/0/3 上。

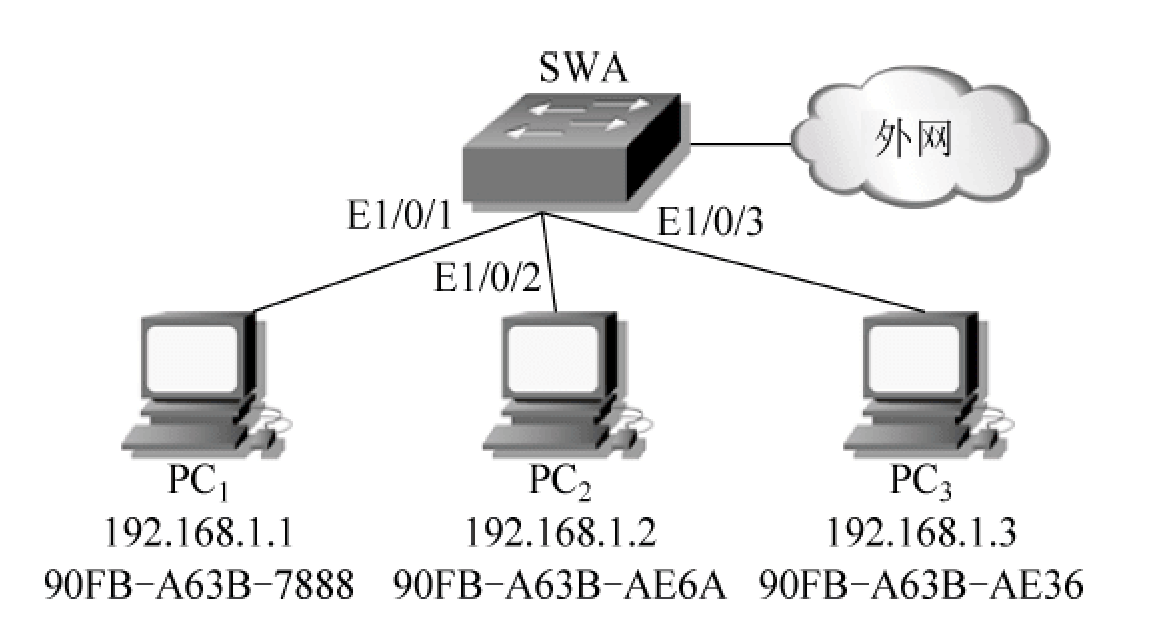


图 6-37 H3C S3610 上端口绑定的配置

具体的配置命令如下：

```
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]user-bind ip-address 192.168.1.1
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]user-bind mac-address 90fb-a63b-ae6a
```

```
[SWA-Ethernet1/0/2]quit
[SWA]interface Ethernet 1/0/3
[SWA-Ethernet1/0/3]user-bind ip-address 192.168.1.3 mac-address 90fb-a63b-ae36
```

配置完成后,使用 display user-bind 命令查看端口绑定信息如下:

```
[SWA]display user-bind
Total entries found: 3
MAC             IP            Vlan   Port             Status
N/A             192.168.1.1   N/A    Ethernet1/0/1    Static
90fb-a63b-ae6a  N/A           N/A    Ethernet1/0/2    Static
90fb-a63b-ae36  192.168.1.3   N/A    Ethernet1/0/3    Static
```

从显示的结果可以看出具体的 IP 地址和 MAC 地址与端口的绑定情况。此时交换机 SWA 的 Ethernet1/0/1、Ethernet1/0/2 和 Ethernet1/0/3 端口上仅允许相应的 PC_1、PC_2 和 PC_3 与外部网络通信,而如果将其他计算机连接到这些端口上,由于相应的 IP 地址或 MAC 地址不匹配,将无法连接外部网络。例如,将 PC_1 的 IP 地址修改为 192.168.1.10,会发现 PC_1 将无法连接外部网络,这是因为在交换机 SWA 的端口 Ethernet1/0/1 收到 PC_1 发来的报文后,会将报文中的源 IP 地址与端口上绑定的 IP 地址进行比较,而端口 Ethernet1/0/1 发现报文源 IP 地址不在自己的绑定表项中,因此会将 PC_1 发来的报文当做非法报文丢弃掉。

需要注意的是:在 H3C S3610 交换机上,相同的 IP 地址 MAC 地址可以在多个端口上进行绑定。例如在上面的例子中,在将 PC_3 的 IP 地址和和 MAC 地址绑定到端口 Ethernet1/0/3 上的同时,还可以将其绑定到端口 Ethernet1/0/4 上。

6.5.2 H3C E126A 上端口绑定的配置

H3C E126A 上端口绑定的配置命令如下:

```
[H3C-Ethernet1/0/1]am user-bind mac-addr mac-address ip-addr ip-address
```

在 H3C E126A 交换机上,只能进行 IP+MAC 的绑定,不支持单独只绑定 IP 地址或单独只绑定 MAC 地址。

在此依然使用如图 6-37 所示的网络,要求将 PC_1、PC_2 和 PC_3 的 IP 地址和 MAC 地址分别绑定到交换机 SWA 的端口 Ethernet1/0/1、Ethernet1/0/2 和 Ethernet1/0/3 上。具体的配置命令如下:

```
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]am user-bind mac-addr 90fb-a63b-7888 ip-addr 192.168.1.1
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]am user-bind mac-addr 90fb-a63b-ae6a ip-addr 192.168.1.2
[SWA-Ethernet1/0/2]quit
[SWA]interface Ethernet 1/0/3
[SWA-Ethernet1/0/3]am user-bind mac-addr 90fb-a63b-ae36 ip-addr 192.168.1.3
```

配置完成后,使用 display am user-bind 命令查看端口绑定信息如下:

```
[SWA]display am user-bind
Following User address bind have been configured:
   Mac                    IP                    Port
   90fb-a63b-7888         192.168.1.1           Ethernet1/0/1
   90fb-a63b-ae6a         192.168.1.2           Ethernet1/0/2
   90fb-a63b-ae36         192.168.1.3           Ethernet1/0/3
Unit 1:Total 3 found, 3 listed.

Total: 3 found.
```

从显示的结果可以看出具体的 IP 地址和 MAC 地址与端口的绑定情况。同样,此时交换机 SWA 的 Ethernet1/0/1、Ethernet1/0/2 和 Ethernet1/0/3 端口上仅允许相应的 PC_1、PC_2 和 PC_3 与外部网络通信。

与 H3C S3610 交换机不同,对于 H3C E126A 交换机而言,对于同一个 MAC 地址和 IP 地址只能在一个端口上进行绑定,如果在多个端口上绑定,系统将会提示错误。例如在上面的例子中,如果将 PC_3 的 IP 地址和 MAC 地址绑定到端口 Ethernet1/0/3 上的同时,再绑定到端口 Ethernet1/0/4 上,系统显示的结果如下:

```
[SWA-Ethernet1/0/4]am user-bind mac-addr 90fb-a63b-ae36 ip-addr 192.168.1.3
The mac address 90fb-a63b-ae36 can not be bound more than one time.
```

注意:如果某端口上配置了端口绑定,则不能配置该端口加入汇聚组;而如果某端口已经加入到了某个汇聚组中,则禁止在该端口上配置端口绑定功能。

6.5.3 Cisco 设备端口绑定的配置

在 Cisco 设备上配置端口绑定功能,分成几种不同的情况,下面分别对其进行介绍。

(1) IP+MAC 的绑定

在 Cisco 设备上配置 IP+MAC 的绑定是在全局模式下进行的,并不会绑定到特定的端口上。具体的配置命令如下:

```
Switch(config)#arp ip-address mac-address arpa
```

(2) MAC+端口的绑定

进行 MAC+端口的绑定,一种方法是通过配置端口安全中的静态安全 MAC 地址来实现,在上一节中已经进行了介绍;另一种方法是通过基于 MAC 地址的扩展访问控制列表来实现,涉及的命令如下:

```
Switch(config)#mac access-list extended acl-name
Switch(config-ext-macl)#permit host mac-address any
Switch(config-ext-macl)#exit
Switch(config)#interface interface-type interface-number
Switch(config-if)#mac access-group acl-name in
```

首先定义一个基于 MAC 地址的扩展 ACL 来允许特定的 MAC 地址访问任意的主机,然后将该 ACL 应用到相应的端口上,从而实现 MAC 与端口的绑定关系。

(3) IP+端口的绑定

IP+端口绑定的配置与MAC+端口绑定的配置类似,同样是通过配置ACL来实现。涉及的命令如下:

```
Switch(config)#ip access-list extended acl-name
Switch(config-ext-nacl)#permit host ip-address any
Switch(config-ext-nacl)#exit
Switch(config)#interface interface-type interface-number
Switch(config-if)#ip access-group acl-name in
```

注意:在MAC+端口的绑定中,配置基于MAC地址的扩展ACL,即MACL;而在IP+端口的绑定中,配置基于IP地址的命名扩展ACL,即NACL。

(4) IP+MAC+端口的绑定

进行IP+MAC+端口的绑定有两种方法,一种方法是将IP+端口的绑定与MAC+端口的绑定结合起来,即分别定义一个基于IP地址的ACL和一个基于MAC地址的ACL,并将其应用到相应的端口上即可实现IP+MAC+端口的绑定;另一种方法是通过ip source binding命令来实现,具体如下:

```
Switch(config)#ip source binding mac-address vlan vlan-id ip-address interface interface-type
interface-number
```

在此依然使用如图6-37所示的网络,要求将PC_1、PC_2和PC_3的IP地址和MAC地址分别绑定到交换机SWA的端口Ethernet1/0/1、Ethernet1/0/2和Ethernet1/0/3上。具体的配置命令如下:

```
SWA(config)#ip source binding 90fb.a63b.7888 vlan 1 192.168.1.1 interface FastEthernet 0/1
SWA(config)#ip source binding 90fb.a63b.ae6a vlan 1 192.168.1.2 interface FastEthernet 0/2
SWA(config)#ip source binding 90fb.a63b.ae36 vlan 1 192.168.1.3 interface FastEthernet 0/3
```

配置完成后,使用show ip source binding命令查看端口绑定信息如下:

```
SWA#show ip source binding
MacAddress          IpAddress        Lease(sec)  Type      VLAN       Interface
------------------  ---------------  ----------  --------  ---------  --------------------
90:FB:A6:3B:AE:6A   192.168.1.2      infinite    static    1          FastEthernet0/2
90:FB:A6:3B:78:88   192.168.1.1      infinite    static    1          FastEthernet0/1
90:FB:A6:3B:AE:36   192.168.1.3      infinite    static    1          FastEthernet0/3
Total number of bindings: 3
```

6.6 DHCP Snooping

通过6.5节的学习,已知可以通过端口绑定技术来增强端口的安全性,实现IP源防护功能。但是静态的配置端口与IP地址之间的绑定之前必须知道该端口上所连接终端的IP地址,而如果终端IP地址是由DHCP动态分配的,则无法提前预知,此时就需要借助DHCP Snooping技术来进行动态绑定。

6.6.1 DHCP Snooping 的功能

DHCP Snooping 实际上是 DHCP 的一项安全特性，它的主要功能如下：

(1) 保证客户端从合法的 DHCP 服务器获取 IP 地址。由于 DHCP 客户端并不对 DHCP 服务器进行验证，因此攻击者可以假冒 DHCP 服务器对客户端进行响应，从而使客户端获得攻击者期望的 IP 地址、默认网关地址以及 DNS 服务器地址，使客户端将数据流量发送到攻击者指定的主机，造成信息的泄露。

DHCP Snooping 通过将连接 DHCP 服务器的端口指定为信任端口，而将其他的端口指定为不信任端口来保证客户端从合法的 DHCP 服务器获取 IP 地址。在信任端口收到 DHCP 报文后会进行正常的转发，而如果在不信任端口上收到了 DHCP 服务器响应的 DHCP-OFFER 报文或者 DHCP-ACK 报文后将会丢弃，从而防止客户端获得错误的 IP 地址。

攻击者一般会首先通过 DoS 攻击使合法的 DHCP 服务器无法提供正常的 DHCP 服务，然后再伪装成 DHCP 服务器来欺骗客户端。因此在设置信任端口的同时，一般会通过在不信任端口上配置 DHCP 报文限速功能来防范基于 DHCP 请求的 DoS 攻击。

(2) 监听 DHCP 报文，记录客户端的 IP 地址与 MAC 地址。DHCP Snooping 通过监听 DHCP-REQUEST 报文和从信任端口上收到的 DHCP-ACK 报文，记录客户端的 MAC 地址以及动态获得的 IP 地址，并将其保存到 DHCP Snooping 绑定表中。

通过读取 DHCP Snooping 绑定表中表项的内容可以生成动态端口绑定表项，从而实现动态 IP 地址与端口的绑定。

6.6.2 DHCP Snooping 的配置

1. H3C 设备配置

H3C 设备上 DHCP Snooping 涉及的配置命令如下：

(1) 启用 DHCP Snooping 功能。

```
[H3C]dhcp-snooping
```

默认情况下，DHCP Snooping 功能处于关闭状态。

(2) 设置信任端口。

```
[H3C-Ethernet1/0/1]dhcp-snooping trust
```

在启用 DHCP Snooping 功能后，在默认情况下，所有的端口均为不信任端口，因此需要将直接或间接连接 DHCP 服务器的端口设置为信任端口。

(3) 配置动态绑定功能。

```
[H3C-Ethernet1/0/1]ip check source {ip-address|mac-address|ip-address mac-address}
```

配置了动态绑定功能后，交换机会根据 DHCP Snooping 绑定表中的记录自动生成动态绑定表项，来实现动态 IP 地址与端口之间的绑定。

需要注意的是，在 H3C E126A 和 H3C S3610 上该命令的配置有一些区别，其中在 H3C E126A 上不支持单独的 MAC 地址绑定。

假设存在如图 6-38 所示的网络,其中交换机 SWA 的型号为 H3C E126A,路由器 RTA 作为 DHCP 服务器,PC_1 和 PC_2 均设置为自动获得 IP 地址。要求在交换机 SWA 上启用 DHCP Snooping 功能,将连接路由器 RTA 的端口 Ethernet1/0/24 设置为信任端口,在连接 PC_1 和 PC_2 的端口 Ethernet1/0/1 和 Ethernet1/0/2 上配置动态绑定功能,使端口 Ethernet1/0/1 和 Ethernet1/0/2 分别只允许 PC_1 和 PC_2 访问外部网络。

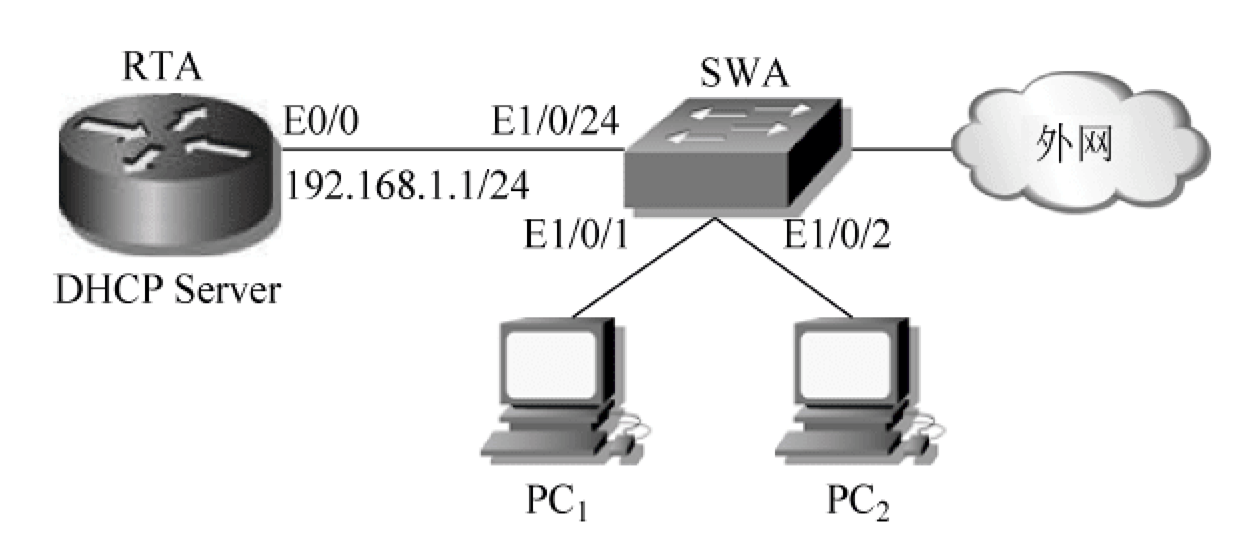


图 6-38 DHCP Snooping 的配置

具体的配置命令如下:

```
[RTA]dhcp enable
[RTA]dhcp server forbidden-ip 192.168.1.1
[RTA]dhcp server ip-pool study
[RTA-dhcp-pool-study]network 192.168.1.0 24
[RTA-dhcp-pool-study]gateway-list 192.168.1.1

[SWA]dhcp-snooping
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]dhcp-snooping trust
[SWA-Ethernet1/0/24]quit
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]ip check source ip-address mac-address
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]ip check source ip-address mac-address
```

配置完成后,在交换机 SWA 上使用 display dhcp-snooping 命令查看 DHCP Snooping 绑定表,显示结果如下:

```
[SWA]display dhcp-snooping
DHCP-Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Unit ID : 1
Type   IP Address     MAC Address     Remaining lease  VLAN  Interface
===  ========  ==========  ===========  ====  ========
---  0 dhcp-snooping item(s) of unit 1 found  ---
```

从显示的结果中可以看出,在 DHCP Snooping 绑定表中没有任何表项,这是因为在配置 DHCP Snooping 之前先配置了 DHCP 服务器,因此在配置 DHCP Snooping 时,PC_1

和 PC_2 已经完成 DHCP 的过程，获得 IP 地址。DHCP Snooping 无法监听到 DHCP-REQUEST 报文和 DHCP-ACK 报文，因此无法获得任何 IP 地址与 MAC 地址的记录。

此时在 PC_1 和 PC_2 上使用 ping 命令测试到达路由器或者外部网络的联通性，发现 PC_1 和 PC_2 根本无法连接路由器和外部网络。这是因为由于 DHCP Snooping 绑定表中没有任何绑定信息，因此交换机 SWA 的端口 Ethernet1/0/1 和 Ethernet1/0/2 会拒绝除 DHCPDISCOVER 和 DHCPREQUEST 报文外的所有数据包。

在 PC_1 和 PC_2 上修复本地连接或者重新启用本地连接，使其进行地址续订或重新开始 DHCP 过程，然后在交换机 SWA 上使用 display dhcp-snooping 命令查看 DHCP Snooping 绑定表，显示结果如下：

```
[SWA]display dhcp-snooping
DHCP-Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Unit ID : 1
Type   IP Address        MAC Address          Remaining lease      VLAN   Interface
===    == === ==         == === ======        === === ===          ==     ==
D      192.168.1.2      90fb-a63b-7888      86227             1      Ethernet1/0/1
D      192.168.1.3      90fb-a63b-ae36      86140             1      Ethernet1/0/2
---    2 dhcp-snooping item(s) of unit 1 found    ---
```

此时在 PC_1 和 PC_2 上使用 ping 命令测试到达路由器或者外部网络的联通性，发现 PC_1 和 PC_2 可以连接路由器和外部网络。如果将 PC_1 或 PC_2 的 IP 地址静态修改为其他的 IP 地址，相应的 PC 将无法连接外部网络，从而验证了动态端口绑定的有效性。

注意：在 H3C E126A 上并不存在单独的动态端口绑定表，而是直接使用 DHCP Snooping 绑定表中的表项来匹配报文的源 IP 地址和源 MAC 地址，实现 IP 源防护功能。

在上面的例子中，如果交换机 SWA 的型号是 H3C S3610，配置命令、测试过程和测试结果与 H3C E126A 完全相同，不同的是在 H3C S3610 上存在单独的动态端口绑定表，当然该表也是从 DHCP Snooping 绑定表中获得的。

当交换机 SWA 使用 H3C S3610 时，在交换机 SWA 上使用 display dhcp-snooping 命令查看 DHCP Snooping 绑定表，显示结果如下：

```
[SWA]display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type      IP Address       MAC Address      Lease      VLAN      Interface
====      == == ===        === =====        ====       = ===     == ==== ==
D         192.168.1.2      90fb-a63b-7888   85576      1         Ethernet1/0/1
D         192.168.1.3      90fb-a63b-ae36   85683      1         Ethernet1/0/2
---    2 dhcp-snooping item(s) found    ---
```

使用 display ip check source 命令查看动态端口绑定表，显示结果如下：

```
[SWA]display ip check source
```

```
Total entries found: 2
MAC              IP            Vlan   Port            Status
90fb-a63b-7888   192.168.1.2   1      Ethernet1/0/1   DHCP-SNP
90fb-a63b-ae36   192.168.1.3   1      Ethernet1/0/2   DHCP-SNP
```

比较上面两条命令显示的结果,可以看出动态端口绑定表学习到了 DHCP Snooping 绑定表中的表项。

2. Cisco 设备配置

在 Cisco 设备上配置 DHCP Snooping 涉及的命令如下。

(1) 启用 DHCP Snooping 功能。

```
Switch(config)#ip dhcp snooping
```

(2) 指定进行 DHCP Snooping 的 VLAN。

```
Switch(config)#ip dhcp snooping vlan {vlanid|vlanid1-vlanid2|vlanid1,vlanid2 …}
```

(3) 设置信任端口。

```
Switch(config-if)#ip dhcp snooping trust
```

(4) 禁用 Option 选项。

```
Switch(config)#no ip dhcp snooping information option
```

在 Cisco 交换机上,一旦启用 DHCP Snooping 功能,默认就会在转发的 DHCP 请求报文中插入 Option 字段信息,这可能会导致 DHCP 失败,因此往往需要禁用 Option 选项。

在此依然使用图 6-38 所示的网络进行 DHCP Snooping 的配置,具体的配置命令如下:

```
RTA(config)#ip dhcp excluded-address 192.168.1.1
RTA(config)#ip dhcp pool study
RTA(dhcp-config)#network 192.168.1.0 255.255.255.0
RTA(dhcp-config)#default-router 192.168.1.1

SWA(config)#ip dhcp snooping
SWA(config)#no ip dhcp snooping information option
SWA(config)#ip dhcp snooping vlan 1
SWA(config)#interface FastEthernet 0/24
SWA(config-if)#ip dhcp snooping trust
```

配置完成后,在交换机 SWA 上使用 show ip dhcp snooping binding 查看 DHCP Snooping 绑定表,显示结果如下:

```
SWA#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
90:FB:A6:3B:78:88   192.168.1.2      86109       dhcp-snooping  1     FastEthernet0/1
90:FB:A6:3B:AE:36   192.168.1.3      86080       dhcp-snooping  1     FastEthernet0/1
Total number of bindings: 2
```

6.7　终端准入控制

终端准入控制(End user Admission Domination,EAD)解决方案从控制用户终端安全接入网络入手,将网络接入控制和用户终端安全策略控制相结合,通过智能客户端、联动设备、安全策略服务器以及第三方软件的联动,对接入网络的用户终端强制实施企业安全策略,并以用户终端对企业安全策略的符合度为条件,控制用户访问网络的接入权限和对网络的使用行为,提高用户终端的主动防御能力,降低病毒、非法访问等安全威胁对网络带来的危害。EAD 解决方案对终端用户的控制过程如图 6-39 所示。

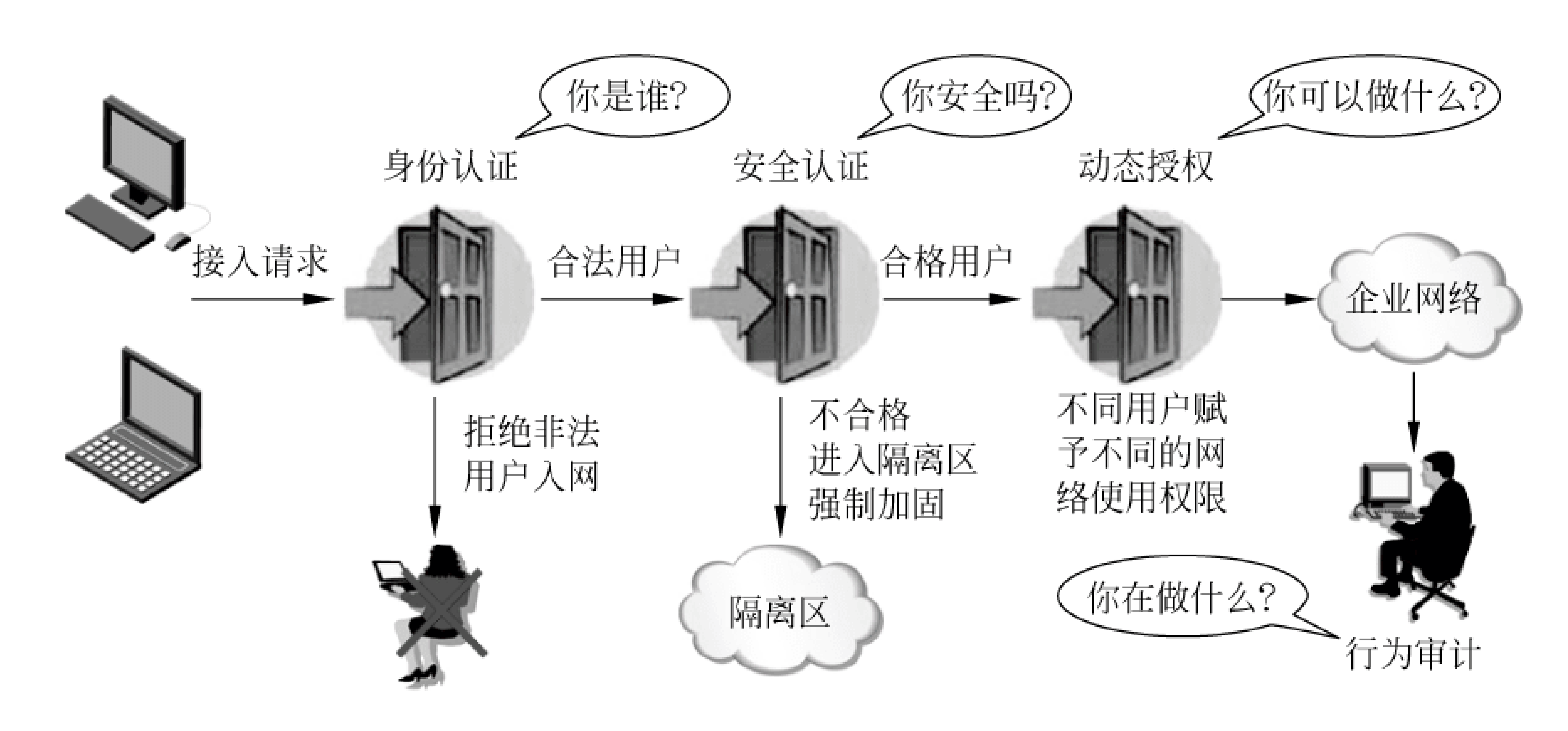


图 6-39　EAD 解决方案示意图

对于需要接入网络的用户,EAD 解决方案首先对其进行身份认证,对于未通过身份认证的非法用户将拒绝其接入网络;对通过身份认证的合法用户进行下一步的安全认证。在安全认证部分根据企业安全策略对用户进行诸如病毒库更新情况、系统补丁安装情况等内容的安全检查,对于安全检查不合格的用户会被放入隔离区进行强制加固,直至满足企业安全策略的要求;对于安全检查合格的用户进入下一步的动态授权。在动态授权部分对不同的用户赋予不同的网络使用权限,使其可以访问网络,并在用户访问网络的过程中对其终端运行情况、网络使用情况等进行审计和监控,及时发现并处理异常行为。

EAD 解决方案组件中包括智能客户端、联动设备、安全策略服务器以及第三方服务器。

(1) 智能客户端:智能客户端即安装了 H3C iNode 智能客户端的用户接入终端,负责身份认证的发起、安全策略的检查以及和安全策略服务器配合进行终端的控制。

(2) 联动设备:联动设备是网络中安全策略的实施点,起到强制用户准入认证、隔离不合格终端、为合法用户提供网络服务的作用。根据应用场合的不同,联动设备可以是交换机、路由器、VPN 网关或无线设备,分别实现不同认证方式(如 IEEE 802.1x、VPN 和 Portal 等)的终端准入控制。针对多样化的网络,EAD 提供了灵活多样的组网方案,联动设备可以根据需要进行灵活部署。

(3) 安全策略服务器:安全策略服务器是 EAD 方案中的管理与控制中心,兼具终端

用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。

(4) 第三方服务器：即补丁服务器、病毒服务器等，被部署在隔离区中。当用户通过身份认证但安全认证失败时，将被隔离到隔离区，此时用户能且仅能访问隔离区中的服务器，通过第三方服务器进行自身安全修复，直到满足安全策略要求。

6.8 模拟公司总部局域网安全配置方案

在本书模拟网络中，AAA 被设计用来实现远程登录局域网内交换机、路由器等网络设备时的集中身份验证、对外连接记账等。其中，网络中有两台 RADIUS 服务器作为 AAA 主备服务器，IP 地址分别为 200.100.8.29/26 和 200.100.8.30/26；RADIUS 共享密钥为“Net&Sec@sjzpc”；用户登录及登录后的对外网络连接事件都要有记账记录；为防止无法连接 RADIUS 服务器导致的远程登录失败，配置备份身份验证方法为 local，并为此配置本地用户名和密码。

模拟公司总部 2 号楼各部门均有一间以上会议室用于召开各类临时会议。由于这些会议室的网络接口所连接主机不固定，无法使用端口绑定 MAC 地址的方式防止非授权的访问，所以对于这些会议室所连接的接入交换机端口，需要通过配置 IEEE802.1x 进行访问控制。

在端口安全配置方面，由于接入交换机物理位置分散，直接连接用户主机，最易受到 MAC 地址欺骗、泛洪攻击，因此在各接入交换机的接入端口上均启用端口安全特性。具体要求如下。

(1) 研发、市场、售后等部网络内有大量移动设备，因此其接入交换机安全端口适合选用动态学习安全 MAC 地址方式；而网络中心、管理、生产等部不应出现大量移动设备，因此其接入交换机安全端口适合选用黏性学习安全 MAC 地址方式。

(2) 为保证接入交换机各安全端口不会接入未经授权的交换机、集线器，各接入交换机安全端口的安全 MAC 地址数目限制为 1 个。

(3) 网络中心、生产部网络要提供网络服务，因此其接入交换机安全端口应配置为限制违规模式，以保证违规行为发生时不会中断网络服务。管理部要求保持网络连接最大可靠性，因此其接入交换机安全端口也应配置为限制违规模式，以保证违规行为发生时不会中断网络连接。研发、市场、售后等部网络在保证网络接入灵活性同时安全风险更大，适宜采用关闭违规模式，提高网络安全系数。

(4) 在配置了安全端口关闭违规模式的交换机上启用 err-disable 计时器可以在指定时间间隔内清除端口的 err-disable 状态，使关闭的端口不需网管员干预就可以再次启用，因此适合于研发、市场、售后等部网络内接入交换机。但 err-disable 计时器不能清除配置文件中的黏滞安全 MAC 地址，因此不适于管理部、网络中心、生产部等网络中的接入交换机。

(5) 除全 0 的 MAC 地址外，各部网络中不应出现的 MAC 地址可根据实际情况设置。

(6) 由于各部接入交换机均设置了安全端口，因此应配置单播、多播泛洪阻塞减少不

必要的流量。

在端口绑定和 DHCP Snooping 方面，由于 DHCP 攻击、IP 欺骗攻击和 ARP 攻击等主要侵犯当地网络，因此在模拟公司总部局域网中的接入交换机、汇聚交换机上，需要配置 DHCP Snooping 和 IPSG 来保障网络通信安全。

目前模拟公司总部网络 IP 地址分配情况为网络中心所有主机及设备均使用静态 IP 地址；其他各部门网络中的网关、服务器使用静态 IP 地址，普通主机使用动态 IP 地址。DHCP 服务器连接在各楼汇聚交换机一侧。

具体的配置要求如下：

(1) 除网络中心外，其他各部门网络 VLAN 中均启用 DHCP 监听，防止假冒 DHCP 响应报文欺骗需动态获得 IP 地址的主机。

(2) 由于网络中的服务器需要使用静态 IP，所以在各接入交换机上需要配置 IP-MAC-端口-VLAN 绑定信息，而其他使用 DHCP 的主机使用 DHCP 监听方式自动生成绑定信息，同时对连接普通主机端口配置 IPSG。

(3) 由于 DHCP 服务器位于汇聚交换机一侧而不是接入交换机，因此下连各接入交换机端口需配置为不可信 DHCP 端口，另外由于 DHCP 广播不能跨越网络，因此汇聚交换机上连核心交换机的端口需配置为可信 DHCP 端口。

(4) 恶意用户或感染了病毒或木马的主机可能通过接入端口攻击网络内其他主机，因此连接各主机的端口配置为 DHCP 不可信端口。

6.9 小结

随着来自网络内部的攻击逐渐增多，局域网安全在网络安全中扮演着越来越重要的角色。为防范以内网主机为跳板的各种攻击，在局域网安全中引入了各种终端接入控制技术，包括 AAA 技术、IEEE 802.1x 技术、端口安全技术、端口绑定技术以及 DHCP Snooping 技术等，每一种技术分别从诸如终端用户身份认证、IP 地址和 MAC 地址认证等不同的方面对终端用户的接入进行安全审查和访问限制，以期保障内部网络的安全。本章对常见的局域网安全技术的原理和配置实现分别进行了介绍，并给出了模拟公司总部局域网的安全配置方案。

6.10 习题

1. AAA 技术中的三个 A 分别代表什么意思？
2. RADIUS 使用传输层哪个协议的哪两个端口进行认证、授权和计费？(　　)
   A. TCP 1645 和 1646　　B. UDP 1645 和 1646
   C. TCP 1812 和 1813　　D. UDP 1812 和 1813
3. 简述受控端口和非受控端口之间的关系以及其各自的作用。
4. 什么是 PAE？设备端 PAE 和客户端 PAE 的作用分别是什么？
5. EAP 信息在 RADIUS 报文中的承载有哪两种方式？其区别是什么？

6. 在端口安全技术中，Intrusion Protection 特性的作用是什么？
7. 端口绑定的目的是什么？
8. 在 DHCP Snooping 中，交换机如何获得端口的动态绑定信息？
9. 在 EAD 中，联动设备一般是什么设备？其作用是什么？

6.11 实训

6.11.1 RADIUS 配置及验证实训

实验学时：2 学时。

每组实验学生人数：4 人。

1. 实验目的

(1) 掌握 RADIUS 服务器的配置。

(2) 掌握 RADIUS 客户端的 RADIUS 方案配置和 AAA 域配置。

(3) 理解 RADIUS 的工作原理和工作流程。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：5 台

(2) 路由器：4 台

(3) 三层交换机：1 台

(4) UTP 电缆：10 条

(5) Console 电缆：5 条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 配置 RADIUS 服务器。

(2) 配置 RADIUS 客户端。

4. 实验指导

(1) 按照图 6-40 所示的网络拓扑结构搭建网络，完成网络连接。其中交换机 SWA 与路由器 RTA、RTB、RTC 和 RTD 分别使用接口 E1/0/1、E1/0/2、E1/0/3 和 E10/4 相连。

(2) 按照图 6-40 所示为路由器、交换机和 PC 配置 IP 地址，其中路由器的 E0/0 接口使用相应网段中的最后一个可用地址，PC_1～PC_4 使用相应网段中第一个可用地址；路由器的 E0/1 接口和相连的交换机 SWA 的接口分别使用相应网段仅有的第一个可用地址和第 2 个可用地址。在 4 台路由器和交换机 SWA 上配置 RIPv2，在交换机 SWA 上配置默认路由并将其引入到 RIPv2 中，保障整个网络的联通性。

H3C 设备参考命令如下：

```
[RTA]interface Ethernet 0/0
[RTA-Ethernet0/0]ip address 10.x.1.30 27
[RTA-Ethernet0/0]quit
[RTA]interface Ethernet 0/1
```

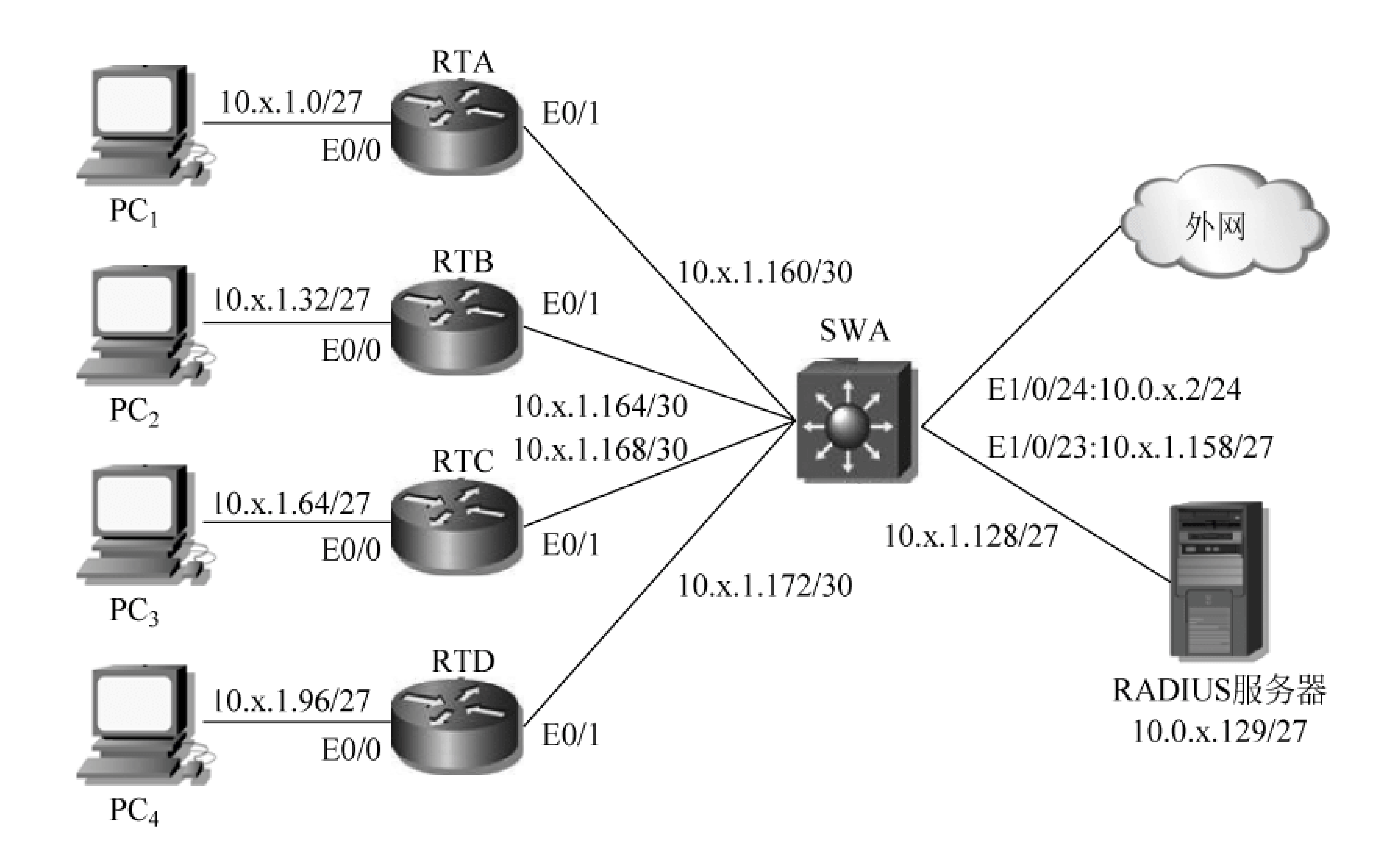


图 6-40 RADIUS 配置及验证实训

```
[RTA-Ethernet0/1]ip address 10.x.1.161 30
[RTA-Ethernet0/1]quit
[RTA]rip
[RTA-rip-1]version 2
[RTA-rip-1]undo summary
[RTA-rip-1]network 10.0.0.0
--------其他 3 台路由器配置略--------
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port link-mode route
[SWA-Ethernet1/0/1]ip address 10.x.1.162 30
[SWA-Ethernet1/0/1]quit
-----接口 Ethernet 1/0/2、Ethernet 1/0/3、Ethernet 1/0/4、Ethernet 1/0/23 和 Ethernet 1/0/24 配置略-----
[SWA]ip route-static 0.0.0.0 0 10.0.x.1
[SWA]rip
[SWA-rip-1]version 2
[SWA-rip-1]undo summary
[SWA-rip-1]network 10.0.0.0
[SWA-rip-1]default-route originate
```

Cisco 设备参考命令如下：

```
RTA(config)#interface FastEthernet 0/0
RTA(config-if)#ip address 10.x.1.30 255.255.255.224
RTA(config-if)#no shutdown
RTA(config-if)#exit
RTA(config)#interface FastEthernet 0/1
RTA(config-if)#ip address 10.x.1.161 255.255.255.252
RTA(config-if)#no shutdown
RTA(config-if)#exit
RTA(config)#router rip
```

```
RTA(config-router)#version 2
RTA(config-router)#no auto-summary
RTA(config-router)#network 10.0.0.0
--------其他 3 台路由器配置略--------

SWA(config)#interface FastEthernet 0/1
SWA(config-if)#no switchport
SWA(config-if)#ip address 10.x.1.162 255.255.255.252
SWA(config-if)#exit
-----接口 FastEthernet 0/2、FastEthernet 0/3、FastEthernet 0/4、FastEthernet 0/23 和 FastEthernet
0/24 配置略-----
SWA(config)#ip routing
SWA(config)#ip route 0.0.0.0 0.0.0.0 10.0.x.1
SWA(config)#router rip
SWA(config-router)#version 2
SWA(config-router)#no aut
SWA(config-router)#no auto-summary
SWA(config-router)#network 10.0.0.0
SWA(config-router)#default-information originate
```

配置完成后,4 台 PC 和 RADIUS 服务器之间互相可以 ping 通,并且均可以连接外部网络。

(3) 配置 RADIUS 服务,使 PC 在远程登录 4 台路由器时使用 RADIUS 进行认证、授权和计费。4 台路由器与 RADIUS 服务器之间的共享密钥均为 testing123,4 台路由器上的 AAA 域名以及用户登录使用的用户名和密码如表 6-6 所示。

表 6-6 RADIUS 认证用户名、密码和 AAA 域名

	AAA 域名	用户名	密码
RTA	network-a	routera	r+a_s1
RTB	network-b	routerb	r+b_s2
RTC	network-c	routerc	r+c_s3
RTD	network-d	routerd	r+d_s4

① 配置 RADIUS 服务器。

在作为 RADIUS 服务器的 PC 上安装 FreeRADIUS.net 软件。安装完毕后,到 C:\FreeRADIUS.net\etc\raddb 目录下,找到配置文件 clients.conf,使用写字板打开,并在文件末尾添加配置信息如下:

```
client 10.x.1.0/24 {
    secret        = testing123
    shortname     = H3C
}
```

注意:在这里 RADIUS 客户端的 IP 地址被设置为一个地址范围 10.x.1.0/24,只要 RADIUS 服务器接收到的 RADIUS 请求中的 NAS-IP 处于该地址范围内,请求就会被处理;另外,shortname 的名称可以是任意值。

在 C:\FreeRADIUS.net\etc\raddb 目录下，找到配置文件 users.conf，使用写字板打开，并在文件开始位置添加配置信息如下：

```
routera@network-a     User-Password == "r+a_s1"
routerb@network-b     User-Password == "r+b_s2"
routerc@network-c     User-Password == "r+c_s3"
routerd@network-d     User-Password == "r+d_s4"
```

注意：如果路由器为 Cisco 设备，则配置文件 users.conf 中的用户名均不携带域名信息。

配置完成后，重新启动 FreeRADIUS 服务，然后在 RADIUS 服务器上使用 netstat -an 命令查看当前的活动端口，应该可以看到 UDP 的 1812 和 1813 端口处于监听状态。

② 配置 RADIUS 客户端。

在此以路由器 RTA 为例进行配置，H3C 设备参考命令如下：

```
[RTA]telnet server enable
[RTA]user-interface vty 0 4
[RTA-ui-vty0-4]authentication-mode scheme
[RTA-ui-vty0-4]quit
[RTA]radius scheme tel
[RTA-radius-tel]primary authentication 10.x.1.129
[RTA-radius-tel]primary accounting 10.x.1.129
[RTA-radius-tel]nas-ip 10.x.1.161
[RTA-radius-tel]key authentication testing123
[RTA-radius-tel]key accounting testing123
[RTA-radius-tel]user-name-format with-domain
[RTA-radius-tel]server-type standard
[RTA-radius-tel]quit
[RTA]domain network-a
[RTA-isp-network-a]authentication login radius-scheme tel
[RTA-isp-network-a]authorization login radius-scheme tel
[RTA-isp-network-a]accounting login radius-scheme tel
[RTA-isp-network-a]accounting optional
[RTA-isp-network-a]quit
[RTA]domain default enable network-a
```

注意：nas-ip 配置的是路由器靠近 RADIUS 服务器的接口 E0/1 的 IP 地址，该地址应包含在 RADIUS 服务器上的配置文件 clients.conf 中定义的 RADIUS 客户端 IP 地址范围中。

Cisco 设备参考命令如下：

```
RTA(config)#aaa new-model
RTA(config)#radius-server host 10.x.1.129 auth-port 1812 acct-port 1813
RTA(config)#radius-server key testing123
```

```
RTA(config)#aaa authentication login tel-authen group radius
RTA(config)#aaa accounting connection tel-acc start-stop group radius
RTA(config)#line vty 0 4
RTA(config-line)#login authentication tel-authen
RTA(config-line)#accounting connection tel-acc
```

路由器RTB、RTC、RTD的配置与路由器RTA的配置类似,在此不再赘述。

配置完成后,在PC_1~PC_4上分别在命令行模式下使用Telnet命令远程登录4台路由器,同时在RADIUS服务器上打开Wireshark软件捕获数据包。此时4台PC使用相应的用户名和密码应该都可以登录到4台路由器。

对RADIUS服务器上捕获的RADIUS数据报文进行分析,查看报文中的相关属性,理解RADIUS的认证、授权和计费流程。

在RADIUS服务器上的C:\FreeRADIUS.net\var\log\radius\radacct目录下,找到四个分别以NAS的IP地址命名的文件夹,每个文件夹下存在3个.log文件,用写字板打开对其内容进行分析。

5. 实验报告

RADIUS服务器配置	clients.conf的配置				
	users.conf的配置				
RTA	VTY的配置				
	RADIUS方案的配置				
	AAA域的配置				
RTB	VTY的配置				
	RADIUS方案的配置				
	AAA域的配置				
RTC	VTY的配置				
	RADIUS方案的配置				
	AAA域的配置				
RTD	VTY的配置				
	RADIUS方案的配置				
	AAA域的配置				
Wireshark捕获的RADIUS报文类型					
RADIUS如何区分计费开始请求包和计费结束请求包?					
在PC上远程登录路由器时,输入的用户名是否需要携带AAA域名信息?为什么?					

6.11.2 IEEE 802.1x配置及验证实训

实验学时:2学时。

每组实验学生人数:4人。

1. 实验目的

(1) 掌握IEEE 802.1x认证服务器的配置。

(2) 掌握 IEEE 802.1x 设备端的配置。

(3) 掌握 IEEE 802.1x 客户端的配置。

(4) 理解 IEEE 802.1x 认证的工作原理和工作流程。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC：5 台

(2) 二层交换机：2 台

(3) 三层交换机：1 台

(4) UTP 电缆：8 条

(5) Console 电缆：3 条

保持所有的交换机均为出厂配置。

3. 实验内容

(1) 配置 IEEE 802.1x 认证服务器。

(2) 配置 IEEE 802.1x 设备端。

(3) 配置 IEEE 802.1x 客户端。

4. 实验指导

(1) 按照图 6-41 所示的网络拓扑结构搭建网络，完成网络连接。

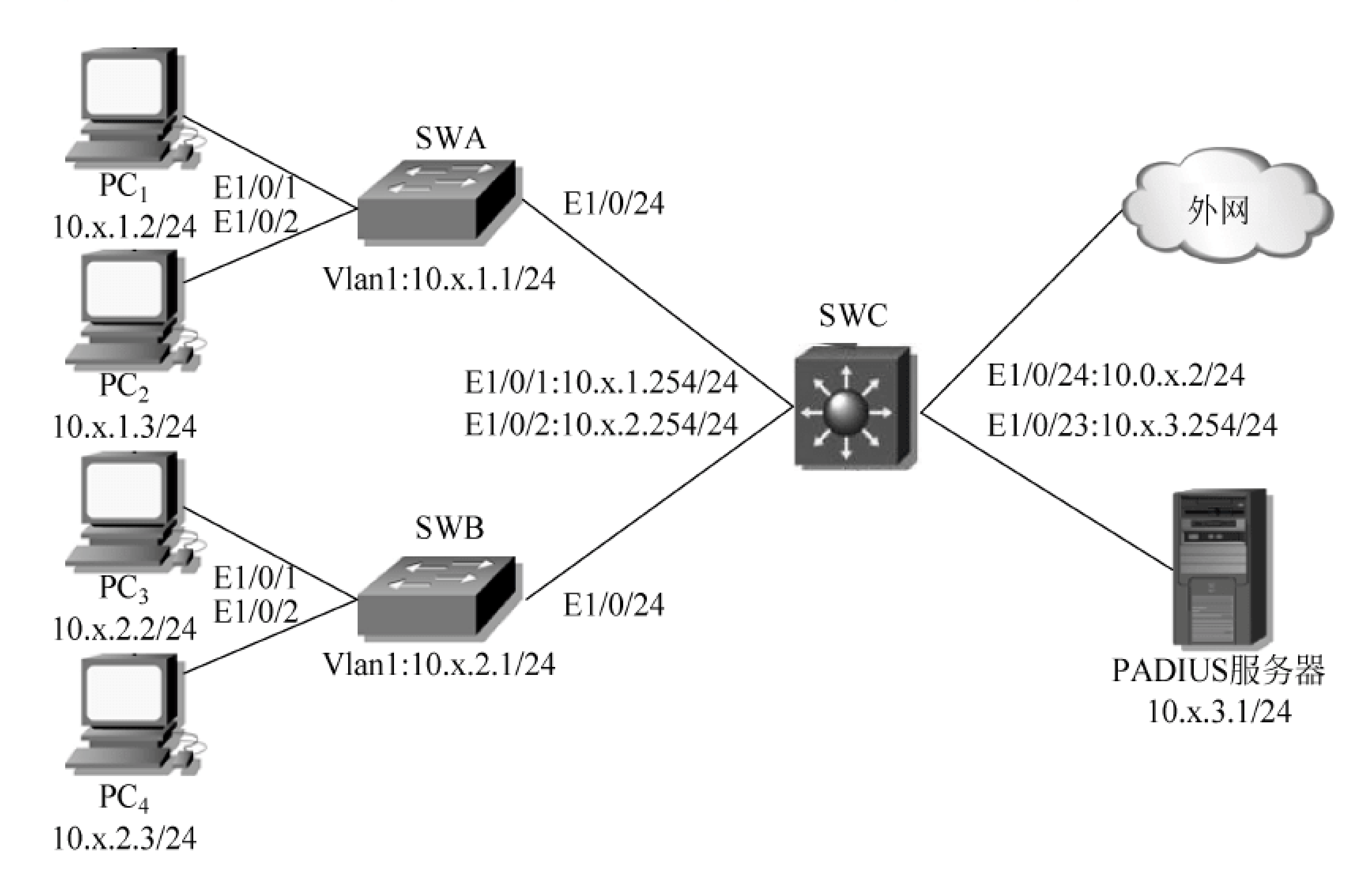


图 6-41　IEEE 802.1x 配置及验证实训

(2) 按照图 6-41 所示为 3 台交换机和 PC 配置 IP 地址，并在 3 台交换机上配置默认路由，实现整个网络的联通性。配置完成后，4 台 PC 和 RADIUS 服务器之间互相可以 ping 通，并且均可以连接外部网络。

(3) 配置 IEEE 802.1x 远端认证，认证方法使用 EAP 终结方式中的 CHAP 认证方法，使 PC_1～PC_4 需要通过认证才可以访问外部网络。交换机 SWA 和 SWB 上配置的 AAA 域名、与 RADIUS 服务器之间的共享密钥以及客户端使用的用户名和密码如表 6-7 所示。

表 6-7 AAA 域名、共享密钥、用户名和密码

	AAA 域名	共享密钥	用户名	密码
SWA	network-a	key123	switcha	s+a_s1
SWB	network-b	testing123	switchb	s+b_s2

① 配置 RADIUS 服务器。在作为 RADIUS 服务器的 PC 上安装 FreeRADIUS. net 软件。安装完毕后,到 C:\FreeRADIUS. net\etc\raddb 目录下,找到配置文件 clients. conf,使用写字板打开,并在文件末尾添加配置信息如下:

```
client 10.x.1.1/24 {
      secret          = key123
      shortname       = SWA
}
client 10.x.2.1/24 {
      secret          = testing123
      shortname       = SWB
}
```

在 C:\FreeRADIUS. net\etc\raddb 目录下,找到配置文件 users. conf,使用写字板打开,并在文件开始位置添加配置信息如下:

```
switcha@network-a      User-Password == "s+a_s1"
switchb@network-b      User-Password == "s+b_s2"
```

注意: 如果交换机为 Cisco 设备,则配置文件 users. conf 中的用户名均不携带域名信息。

配置完成后,重新启动 FreeRADIUS 服务,然后在 RADIUS 服务器上使用 netstat -an 命令查看当前的活动端口,应该可以看到 UDP 的 1812 和 1813 端口处于监听状态。

② 配置设备端。在此以交换机 SWA 为例进行配置,H3C 设备参考命令如下:

```
[SWA]dot1x
[SWA]undo dot1x handshake enable
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]dot1x
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]dot1x
[SWA-Ethernet1/0/2]quit
[SWA]radius scheme lan-acc
[SWA-radius-lan-acc]primary authentication 10.x.3.1 1812
[SWA-radius-lan-acc]primary accounting 10.x.3.1 1813
[SWA-radius-lan-acc]nas-ip 10.x.1.1
[SWA-radius-lan-acc]key authentication key123
[SWA-radius-lan-acc]key accounting key123
[SWA-radius-lan-acc]user-name-format with-domain
[SWA-radius-lan-acc]server-type standard
[SWA-radius-lan-acc]quit
[SWA]domain network-a
```

```
[SWA-isp-network-a]authentication radius-scheme lan-acc
[SWA-isp-network-a]accounting radius-scheme lan-acc
[SWA-isp-network-a]accounting optional
[SWA-isp-network-a]quit
[SWA]domain default enable network-a
```

Cisco 设备参考配置如下：

```
SWA(config)#aaa new-model
SWA(config)#radius-server host 10.x.3.1 auth-port 1812 acct-port 1813
SWA(config)#radius-server key key123
SWA(config)#aaa authentication dot1x default group radius
SWA(config)#dot1x system-auth-control
SWA(config)#interface FastEthernet 0/1
SWA(config-if)#switchport mode access
SWA(config-if)#dot1x port-control auto
SWA(config-if)#dot1x pae authenticator
SWA(config-if)#exit
SWA(config)#interface FastEthernet 0/2
SWA(config-if)#switchport mode access
SWA(config-if)#dot1x port-control auto
SWA(config-if)#dot1x pae authenticator
```

③ 配置客户端。客户端使用 Windows XP 自带的客户端软件或者使用 H3C 的 iNode 客户端软件均可，具体的配置方法请参考 6.3.3 小节。

配置完成后，在 PC_1 ～ PC_4 上分别在客户端软件中输入用户名和密码，启动 IEEE 802.1x 认证过程，同时在 4 台 PC 和 RADIUS 服务器上开启 Wireshark 捕获数据报文。

认证成功后，PC_1 ～ PC_4 即可访问外部网络资源。

对比 PC_1 ～ PC_4 上捕获的 EAPOL 报文和 RADIUS 服务器上捕获的 RADIUS 报文，查看 EAP-Request/MD5-Challenge 报文和 EAP-Response/MD5-Challenge 报文中 Value 属性的值以及 RADIUS Access-Request 报文中的 CHAP-Password 和 CHAP-Challenge 属性的值，理解 EAP 终结方式的认证流程。

5. 实验报告

RADIUS 服务器配置	clients.conf 的配置			
	users.conf 的配置			
SWA	IEEE 802.1x 的配置			
	RADIUS 方案的配置			
	AAA 域的配置			
SWB	IEEE 802.1x 的配置			
	RADIUS 方案的配置			
	AAA 域的配置			
PC_1 认证	EAP-Request/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Challenge 的值	
	EAP-Response/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Password 的值	

续表

PC$_2$ 认证	EAP-Request/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Challenge 的值	
	EAP-Response/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Password 的值	
PC$_3$ 认证	EAP-Request/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Challenge 的值	
	EAP-Response/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Password 的值	
PC$_4$ 认证	EAP-Request/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Challenge 的值	
	EAP-Response/MD5-Challenge 报文 Value 的值		RADIUS Access-Request 报文 CHAP-Password 的值	

6.11.3 端口安全与端口绑定配置及验证实训

实验学时：2学时。

每组实验学生人数：4人。

1. 实验目的

(1) 掌握端口安全的配置和验证方法。

(2) 掌握端口绑定的配置和验证方法。

2. 实验环境

(1) 安装有TCP/IP协议的Windows系统PC：5台

(2) 二层交换机：2台

(3) 三层交换机：1台

(4) UTP电缆：8条

(5) Console电缆：2条

保持所有的交换机均为出厂配置。

3. 实验内容

(1) 配置端口安全功能。

(2) 配置IP地址、MAC地址与端口的绑定。

4. 实验指导

(1) 按照图6-42所示的网络拓扑结构搭建网络，完成网络连接。

(2) 按照图6-42所示为5台PC配置IP地址，网关均为10.0.x.1。配置完成后，PC$_1$～PC$_4$均可以连接外部网络。

(3) 在交换机SWA和SWB上启用端口安全功能，将两台交换机上的端口Ethernet1/0/1和Ethernet1/0/2配置为最多允许两个用户接入；配置端口的安全模式为autolearn；配置Intrusion Protection特性为暂时关闭端口，关闭时间为30s。在此以交换机SWA为例进行配置，H3C设备参考命令如下：

```
[SWA]port-security enable
```

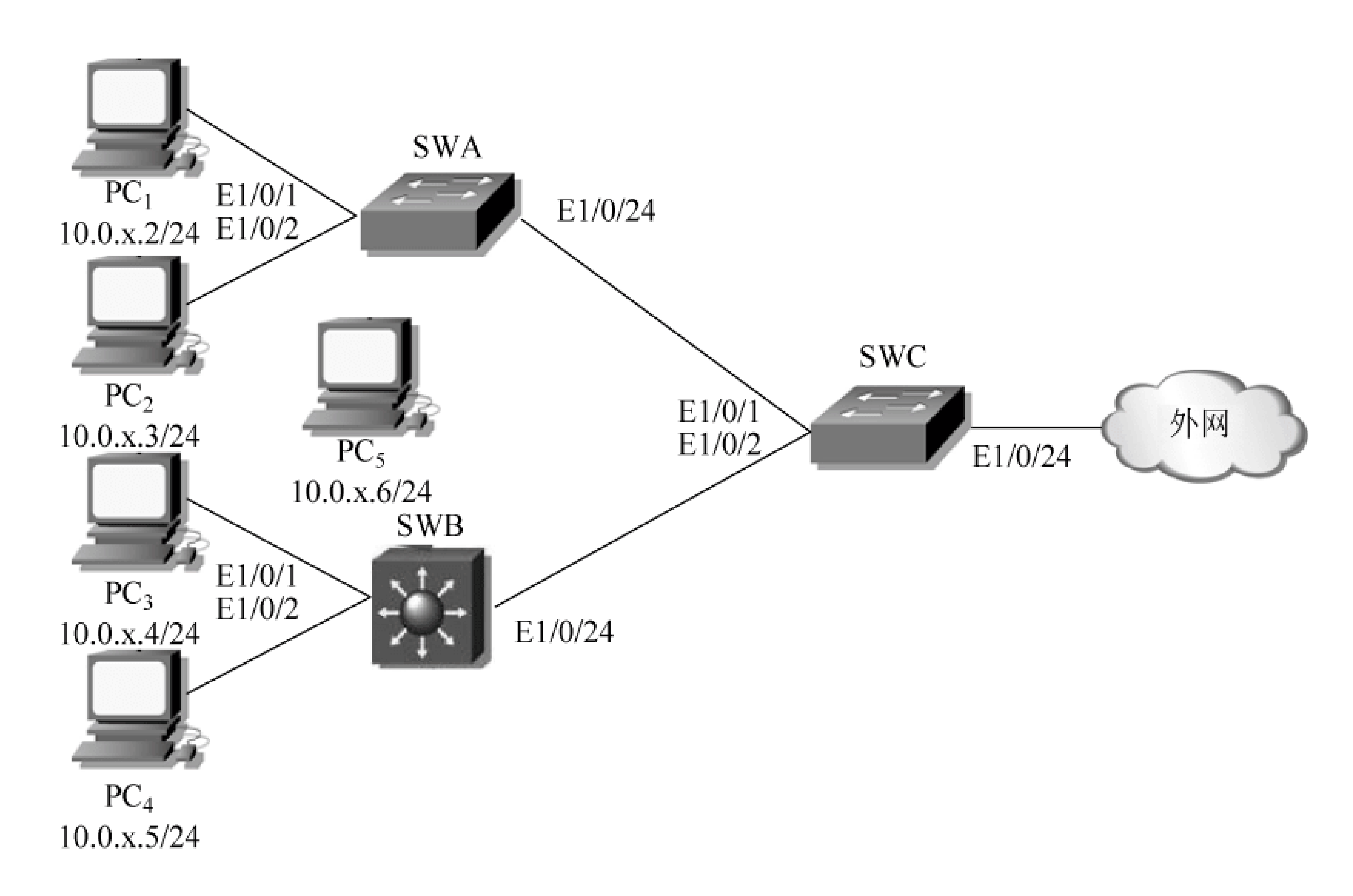


图 6-42 端口安全与端口绑定配置及验证实训

```
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port-security max-mac-count 2
[SWA-Ethernet1/0/1]port-security port-mode autolearn
[SWA-Ethernet1/0/1]port-security intrusion-mode disableport-temporarily
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]port-security max-mac-count 2
[SWA-Ethernet1/0/2]port-security port-mode autolearn
[SWA-Ethernet1/0/2]port-security intrusion-mode disableport-temporarily
[SWA-Ethernet1/0/2]quit
[SWA]port-security timer disableport 30
```

Cisco 设备参考命令如下：

```
SWA(config)#interface range FastEthernet 0/1 - 2
SWA(config-if-range)#switchport mode access
SWA(config-if-range)#switchport port-security
SWA(config-if-range)#switchport port-security maximum 2
SWA(config-if-range)#switchport port-security mac-address sticky
SWA(config-if-range)#switchport port-security violation shutdown
SWA(config-if-range)#exit
SWA(config)#errdisable recovery cause psecure-violation
SWA(config)#errdisable recovery interval 30
```

配置完成后，在 PC_1～PC_4 上使用 ping 命令连接外部网络，使交换机的相应端口可以学习到 PC 的 MAC 地址。然后分别在交换机 SWA 和 SWB 上使用 display port-security 或者 show port-security 命令查看相应端口安全配置信息，使用 display mac-address security、display port-security mac-address security 或者 show port-security address 命令查看交换机学习到的安全 MAC 地址的信息。

将 PC_1 和 PC_2 互换端口,将 PC_3 和 PC_4 互换端口,然后在 PC_1～PC_4 上使用 ping 命令连接外部网络,发现 4 台 PC 均无法连接外部网络,在交换机 SWA 和 SWB 上使用 display port-security 或者 show port-security 命令查看相应的端口安全配置信息,会发现端口状态为 link-up,端口的安全模式依然为 autolearn,学习到的安全 MAC 地址数也依然为 1;使用 display mac-address security、display port-security mac-address security 或者 show port-security address 命令查看交换机学习到的安全 MAC 地址信息,会发现在相应的端口上并不会学习到后连接 PC 的 MAC 地址,例如,在交换机 SWA 的端口 Ethernet1/0/1 上不会学习到 PC_2 的 MAC 地址。这是因为在同一个 VLAN 中,一个安全 MAC 地址只能被添加到一个端口上,由于 PC_2 的 MAC 地址已经被交换机 SWA 的端口 Ethernet1/0/2 学习到,因此端口 Ethernet1/0/1 将不会再将 PC_2 的 MAC 地址添加到自己的安全 MAC 地址中。

将 PC_1 和 PC_2 分别连接到交换机 SWB 的 Ethernet1/0/1 和 Ethernet1/0/2 端口上,将 PC_3 和 PC_4 分别连接到交换机 SWA 的 Ethernet1/0/1 和 Ethernet1/0/2 端口上,然后在 PC_1～PC_4 上使用 ping 命令连接外部网络,此时发现 4 台 PC 均可以连接外部网络。在交换机 SWA 和 SWB 上使用 display port-security 或者 show port-security 命令查看相应的端口安全配置信息,会发现端口的安全模式变为 secure,学习到的安全 MAC 地址数变为 2;使用 display mac-address security、display port-security mac-address security 或者 show port-security address 命令查看交换机学习到的安全 MAC 地址信息,会发现相应端口学习到了现在连接 PC 的 MAC 地址。

将 PC_5 连接到交换机 SWA 或 SWB 上的 Ethernet1/0/1 或 Ethernet1/0/2 端口,并在 PC_5 上使用 ping 命令连接外部网络,会发现 PC_5 无法连接外部网络。使用 display port-security 或者 show port-security 命令查看相应的端口安全配置信息,会发现端口状态变为 link-down。将原来的 PC 重新连接到相应的端口,会发现经过 30s 以后端口将重新回到 UP 状态。

(4) 将交换机 SWA 和 SWB 重新启动以清空端口安全的配置,将网络物理连接恢复到图 6-41 所示的连接状态。

(5) 在交换机 SWA 和 SWB 的端口 Ethernet1/0/1 和 Ethernet1/0/2 上分别绑定所连接 PC 的 IP 地址和 MAC 地址。H3C 设备参考命令如下:

```
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]am user-bind mac-addr 90fb-a63b-7888 ip-addr 10.0.x.2
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]am user-bind mac-addr 90fb-a63b-ae6a ip-addr 10.0.x.3

[SWB]interface Ethernet 1/0/1
[SWB-Ethernet1/0/1]user-bind ip-address 10.0.x.4 mac-address 90fb-a63b-ae36
[SWB-Ethernet1/0/1]quit
[SWB]interface Ethernet 1/0/2
[SWB-Ethernet1/0/2]user-bind ip-address 10.0.x.5 mac-address 90fb-a63b-1d12
//注意:以上配置中的 MAC 地址需要根据实际 PC 的 MAC 地址做出修改
```

Cisco 设备参考命令如下：

```
SWA(config)#ip source binding 90fb.a63b.7888 vlan 1 10.0.x.2 interface FastEthernet 0/1
SWA(config)#ip source binding 90fb.a63b.ae6a vlan 1 10.0.x.3 interface FastEthernet 0/2

SWB(config)#ip source binding 90fb.a63b.ae36 vlan 1 10.0.x.4 interface FastEthernet 0/1
SWB(config)#ip source binding 90fb.a63b.ae6a vlan 1 10.0.x.5 interface FastEthernet 0/2
//注意：以上配置中的 MAC 地址需要根据实际 PC 的 MAC 地址做出修改
```

配置完成后，使用 display am user-bind、display user-bind 或者 show ip source binding 命令查看相应的端口绑定信息。

此时，在 PC_1～PC_4 上使用 ping 命令均可以连接外部网络。将 PC_1 和 PC_2 互换端口，将 PC_3 和 PC_4 互换端口，再次使用 ping 命令连接外部网络，会发现 4 台 PC 均无法连接外部网络，从而验证了端口绑定的作用。

5. 实验报告

<table>
<tr><td rowspan="6">端口安全</td><td>SWA 的配置</td><td colspan="4"></td></tr>
<tr><td>SWB 的配置</td><td colspan="4"></td></tr>
<tr><td rowspan="2">PC_1/PC_3 与 PC_2/PC_4 互换端口</td><td>PC 能否连接外部网络</td><td></td><td>端口能否学习到新 MAC 地址</td><td></td></tr>
<tr><td>分析原因</td><td colspan="3"></td></tr>
<tr><td rowspan="2">PC_5 连接到某端口</td><td>PC_5 能否连接外部网络</td><td></td><td>端口状态</td><td></td></tr>
<tr><td>分析原因</td><td colspan="3"></td></tr>
<tr><td rowspan="4">端口绑定</td><td>SWA 的配置</td><td colspan="4"></td></tr>
<tr><td>SWB 的配置</td><td colspan="4"></td></tr>
<tr><td rowspan="2">PC_1/PC_3 与 PC_2/PC_4 互换端口</td><td>PC 能否连接外部网络</td><td colspan="3"></td></tr>
<tr><td>分析原因</td><td colspan="3"></td></tr>
</table>

第 7 章

网络管理技术

本章任务：根据工程任务安全需求分析，解决计算机网络的管理问题。

必备知识：(1) 网络管理体系架构。

(2) SNMP 协议。

(3) 网络配置管理。

(4) 网络故障管理。

(5) 网络安全管理。

(6) 网络性能管理。

(7) 网络计费管理。

学习目标：完成模拟公司总部局域网的网络管理任务。

7.1 模拟公司网络管理任务分析

由于模拟公司大部分生产、办公系统依赖于公司的计算机网络，因此对网络进行有效管理，保障网络安全、可靠、高效运行非常重要。模拟公司网络管理任务主要包括以下几点。

(1) 在相关网络管理软件协助下，及时了解网络拓扑结构的变化，包括网络内路由器、三层交换机、接入层交换机之间，与其他设备之间的物理连接关系，局域网划分、VLAN 划分等。

(2) 在相关网络管理软件协助下，及时检测广域网线路各条线路的流量，统计过去任何一段时间，任何一条线路的输入、输出、总流量以及丢包率、错包率；以实时更新的流量统计方式对网络流量状况进行监测；能统计各线路丢包率、错包率，为线路性能的分析提供科学依据。

(3) 在相关网络管理软件协助下，及时发现网络故障发生点。记录网络设备、线路、终端、病毒、非法入网、违规操作、相关告警设置等各种严重和一般告警信息。

(4) 在相关网络管理软件协助下，进行设备的配置管理。

(5) 在相关网络管理软件协助下，进行日志管理，分门别类记录网络的各种故障；对网络的各类运行情况进行统计，掌握网络动态。

(6) 在相关网络管理软件协助下，进行安全管理。例如，对使用 Internet 线路的网络

连接使用加密技术进行保护，定期对网络进行安全审计等。

7.2　网络管理技术基础

随着网络技术的发展和网络规模的不断扩大，传统上的网络管理员对网络设备进行分布式手工管理的网络管理方式已经无法满足网络管理的需求。网络管理技术通过对网络管理的标准、功能以及体系结构进行定义，由基于网络管理标准开发的网络管理系统为大中型网络中的网络设备提供统一的管理平台，实现对网络的集中维护、远程监控等功能，从而提高网络管理的效率，实现智能化的网络管理。

7.2.1　网络管理的功能

网络管理就是通过对网络的运行状态进行检测和控制，使其能够有效、可靠、安全和经济地运行。国际标准化组织（International Organization for Standardization，ISO）在 ISO/IEC 7498-4 文档中将网络管理的功能划分为 5 个方面，分别是故障管理（Fault Management）、配置管理（Configuration Management）、计费管理（Accounting Management）、性能管理（Performance Management）和安全管理（Security Management），简称为 FCAPS，如图 7-1 所示。

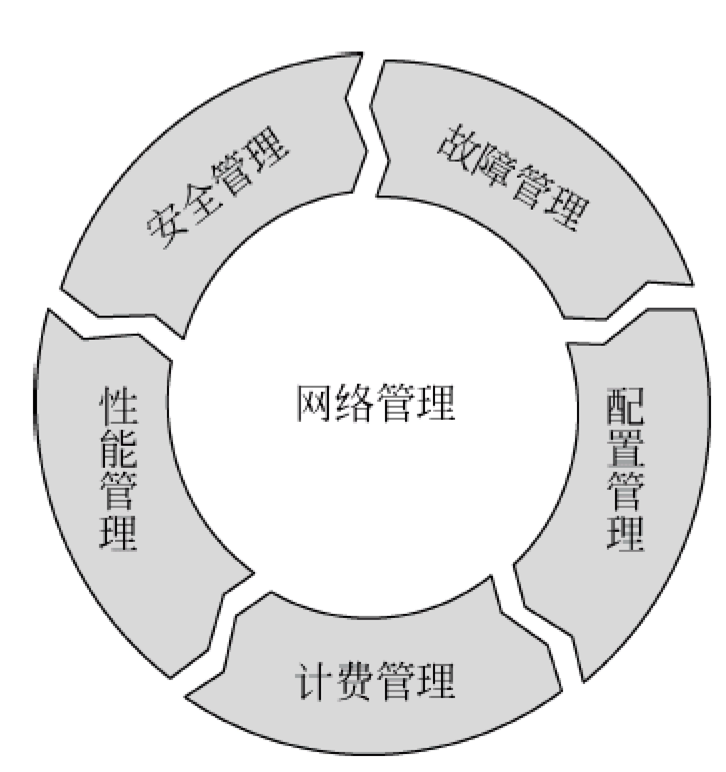


图 7-1　网络管理功能划分

1. 故障管理

故障管理通过对网络中的故障进行检测、隔离、报告和修复来保障网络组件的稳定性、可用性和可服务性。故障管理通过检测网络中的异常事件来发现故障；通过日志来记录故障的情况；根据故障的现象采取相应的跟踪、诊断和测试措施，进而修复故障。故障管理包含的典型功能如下：

（1）检测被管设备的故障现象，接收被管设备的故障事件报告。

（2）执行诊断测试，确定故障的位置和性质。

（3）当存在备用设备或迂回路由时，提供新的网络资源用于服务。

（4）通过设备的维护或更换等措施进行故障的修复。

（5）维护故障日志文件，记录故障信息，分析故障原因。

2. 配置管理

配置管理用来初始化并配置网络，以使其能够提供网络服务。配置管理可以标识并收集被管设备的配置信息，监控网络当前配置并可根据需求修改当前配置，启动或关闭资源等。配置管理包含的典型功能如下：

（1）初始化或关闭被管设备。

（2）收集网络当前的配置信息。

（3）根据要求修改网络的配置信息。

(4) 存取网络配置信息。

(5) 发现和显示网络的拓扑结构。

(6)按照要求生成配置报告。

3. 计费管理

计费管理负责监视和记录用户对网络资源的使用情况,并根据使用情况计算所需要的成本和费用,以作为向用户收费的依据。计费管理对公共商业网络显得尤为重要。计费管理包含的典型功能如下:

(1) 统计网络利用率等效益数据,为网络运营部门提供制定资费政策的依据。

(2) 记录用户使用网络资源的情况,并以此为依据计算用户费用。

(3) 保存计费信息,以备用户查询和质疑。

4. 性能管理

性能管理负责监测网络的性能,通过监测网络中的吞吐量、利用率、错误率以及响应时间等指标数据,分析网络的运行趋势、验证网络的服务水平、找出潜在的问题,将网络性能控制在一个可以接受的水平。性能管理的目的就是保证网络能够提供可靠和连续地服务。性能管理包含的典型功能如下:

(1) 从被管设备中收集和统计与性能相关的数据,并产生相应的记录。

(2) 分析性能数据、检测性能故障、产生性能告警报告。

(3) 预测性能的长期变化趋势。

(4) 控制被管设备,保证网络的性能指标。

5. 安全管理

安全管理负责保护网络资源的安全,包括限制非法入侵者进入网络的进网安全防护;检查用户访问权限的应用访问安全防护;对数据进行加密和认证的网络传输信息的安全防护等。安全管理包含的典型功能如下:

(1) 管理用户口令、密钥以及访问权限等安全措施信息,并依据安全措施信息判断和拒绝非法操作。

(2) 进行安全审查,检查网络中各种潜在的安全漏洞。

(3) 对影响网络安全的事件进行记录,生成安全报告。

(4) 维护安全日志文件。

7.2.2 网络管理模型

在网络管理中,一个网络中的网络设备、服务器、主机等将均被看做被管理的对象,而由某一台运行网络管理软件的主机作为管理者对其进行管理,在管理者和被管理的对象之间会遵循一定的规则进行通信,而通信的目的是管理者可以对被管理的对象上的资源信息进行查询和修改。因此,典型的网络管理模型应该由 4 部分组成,分别是网络管理实体(Network Management Entity,NME)、网络管理代理(Network Management Agent,NMA)、网络管理协议(Network Management Protocol,NMP)和管理信息库(Management Information Base,MIB),如图 7-2 所示。

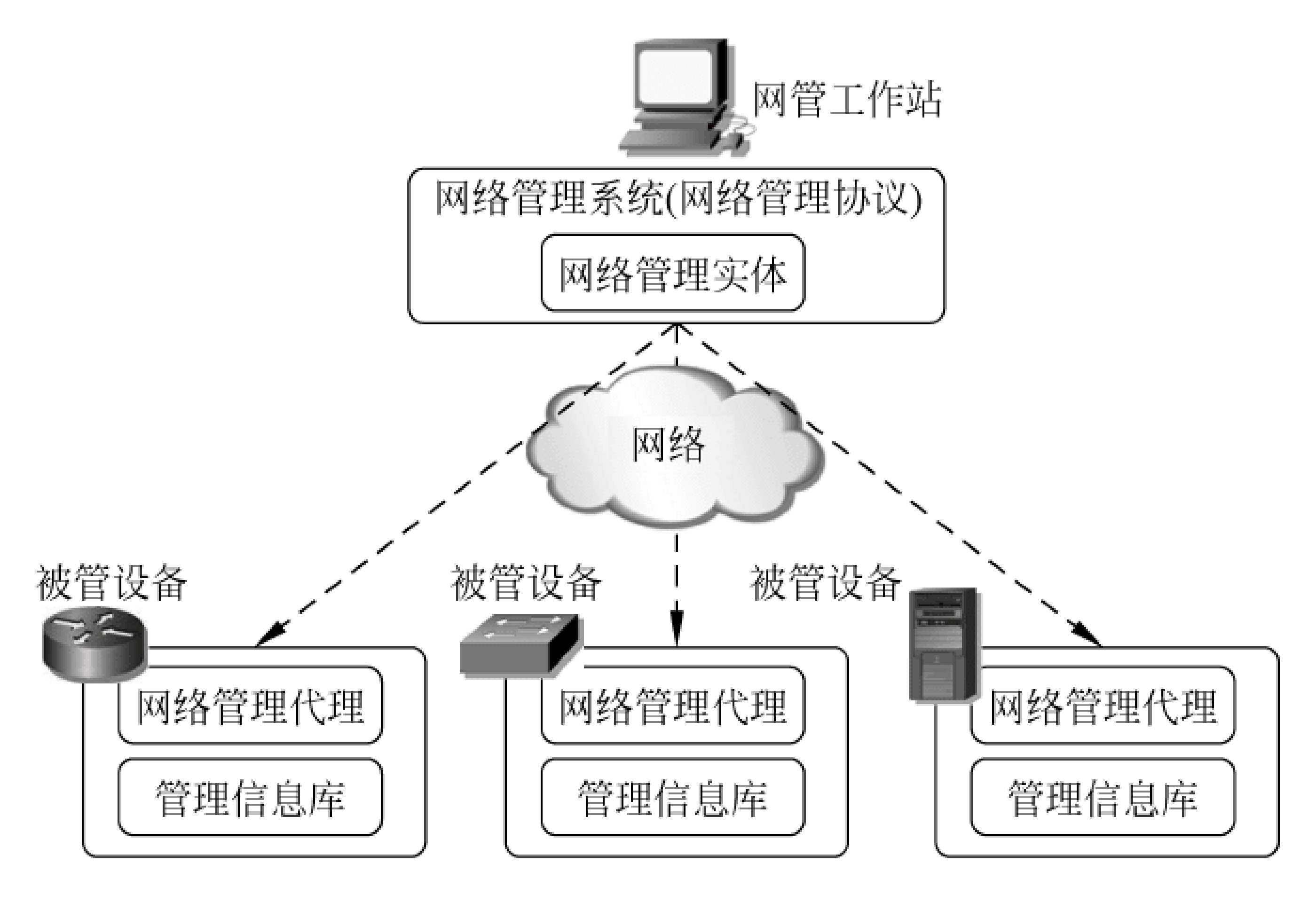


图 7-2　网络管理模型

1. 网络管理实体

网络管理实体即网络管理系统进程,它向运行在被管理的网络设备上的网络管理代理程序发出管理操作指令,并接收来自网络管理代理的信息,以对各种网络设备、网络资源进行监控和管理。

运行网络管理系统的主机称为网管工作站,网管工作站一般采用专门的服务器来实现,逻辑上位于网络的主干或接近主干的位置。

2. 网络管理代理

网络管理代理是驻留在网络设备上的与网络管理实体之间进行交互的进程,它接收来自网络管理实体的指令,根据指令要求对被管理设备上的管理信息库中的相关信息进行读取和修改操作,并将相应的信息返回给网络管理实体。网络管理代理也可以将自身系统中发生的事件主动通知给网络管理实体。网络管理代理可以被看做是网络管理实体与被管设备上的管理信息库之间的中介。

3. 网络管理协议

网络管理协议是网络管理实体与网络管理代理之间进行通信所遵守的约定和规则。目前最有影响的两个网络管理协议分别是国际标准化组织定义的公共管理信息服务和公共管理信息协议(Common Management Information Services/Common Management Information Protocol,CMIS/CMIP)以及互联网工程任务组(Internet Engineering Task Force,IETF)定义的简单网络管理协议(Simple Network Management Protocol,SNMP)。其中 CMIS/CMIP 较为有限的应用在基于 OSI 的网络中,而 SNMP 广泛应用在基于 TCP/IP 的网络中。

4. 管理信息库

管理信息库是被管理对象的信息集合。任何一个被管理的资源都可以表示成为一个对象,称为被管理对象,被管理对象在某一时刻的值称为管理变量或被管对象的实例,所

以管理信息库实际上就是各种管理变量的集合,它反映了被管理对象在系统中的状态。每一个被管理的设备上都有自己的管理信息库,管理信息库由被管设备上的网络管理代理进程负责管理和维护,维持其与物理实体之间的一致性。

7.3 简单网络管理协议

7.3.1 SNMP基础

SNMP协议由IETF于1988年发布,其前身是简单网关管理协议(Simple Gateway Management Protocol,SGMP)。与网络管理模型相对应,SNMP的结构分为SNMP管理者和SNMP代理两部分。每一个支持SNMP的网络设备中都包含一个SNMP代理,它随时记录网络设备的各种信息,SNMP管理者再通过SNMP协议查询或修改SNMP代理所记录的信息。SNMP协议的基本工作原理就是使SNMP管理者通过轮询SNMP代理,以及SNMP代理主动向SNMP管理者发送陷阱信息,来设置一些被管对象的属性和监控一些网络事件的发生,从而达到网络管理的目的。

在SNMP协议中,SNMP管理者从SNMP代理获得被管对象信息的途径有两种:轮询和自陷。轮询是指SNMP管理者周期性地向网络中的各个SNMP代理发送查询命令来获得被管设备上各个被管对象的数据信息。通过轮询,SNMP管理者可以对网络的整体情况进行监控,但是轮询存在无法确保被管对象数据信息实时性的缺陷,尤其对于网络故障信息的实时性监控。由于轮询是周期性的,因此轮询时间间隔的大小将对轮询的结果产生影响。如果轮询的时间间隔太小,则会产生太多不必要的通信流量;而如果轮询的时间间隔太大,则对于网络中的故障事件又可能会无法及时监控到。为解决轮询存在的缺陷,对于故障等异常事件采用自陷的方式,即在网络中出现了异常事件的时候,相应的SNMP代理会主动向SNMP管理者发送陷阱报文,而不必等到SNMP管理者对其进行轮询,从而使SNMP管理者可以实时监控到这些故障信息。轮询和自陷两种方法的结合称为面向自陷的轮询方法(Trap-directed Polling)。

为防范恶意攻击者冒充SNMP管理者对SNMP代理进行操作,在SNMP协议中,SNMP管理者与SNMP代理之间使用团体名(Communtiy Name)进行认证。只有SNMP管理者与SNMP代理使用的团体名相同,SNMP管理者才能对SNMP代理进行管理,否则SNMP代理将向SNMP管理者发送认证失败信息,并丢弃相关的管理报文。

SNMP协议经过二十余年的发展,目前包含SNMPv1、SNMPv2和SNMPv3共3个版本。在SNMPv1中,为SNMP管理者与SNMP代理之间的交互定义了5种不同类型的PDU,分别如下。

(1) Get-Requset:由SNMP管理者发送给SNMP代理,用于从SNMP代理处获取指定被管理对象的值。

(2) Get-Next-Request:由SNMP管理者发送给SNMP代理,用于从SNMP代理处获取指定被管理对象的下一个对象的值。Get-Next-Request还可以通过遍历MIB树来连续获取一组被管理对象的值。

(3) Set-Requset:由SNMP管理者发送给SNMP代理,用于设置SNMP代理处指

定被管理对象的值。

(4) Get-Response：由 SNMP 代理发送给 SNMP 管理者，是对 Get-Requset、Get-Next-Request 和 Set-Requset 的响应报文，用于返回请求值或错误类型等信息。

(5) Trap：由 SNMP 代理发送给 SNMP 管理者，用于向 SNMP 管理者发送非请求信息，一般用来通告 SNMP 代理处有重要事件的发生，即异常报警等。

作为应用层协议，SNMP 协议在传输层基于 UDP 协议来实现，其中 SNMP 管理者在 UDP 的 162 端口上监听来自 SNMP 代理的 Trap 报文，而 SNMP 代理则在 UDP 的 161 端口上监听来自 SNMP 管理者的各种 Requset 报文。

随着网络规模的扩大和网络技术的发展，SNMPv1 已逐渐无法满足网络管理的需求，主要表现在以下两个方面。

(1) SNMPv1 只支持集中式的网络管理，即在网络中只有一个 SNMP 管理者。在网络规模较大时，将造成 SNMP 管理者的负担过重，并且由于所有的管理流量均汇集到 SNMP 管理者处，造成管理流量的拥塞，影响网络管理的效率。

(2) SNMPv1 的安全性较差，所有的信息均采用明文方式传送，缺乏必要的加密、认证等手段，无法保证数据的机密性以及完整性。

为解决 SNMPv1 存在的问题，在 1993 年发布了 SNMP 的第 2 版，即 SNMPv2。SNMPv2 对 SNMPv1 进行了修订，并在性能、安全等方面进行了改进，但 SNMPv2 中的新安全特性被认为过于复杂而未被广泛接受。因此在 1996 年发布了 SNMPv2c (Community-based SNMP)，即基于团体名的 SNMP 第 2 版。SNMPv2c 包含了 SNMPv2 除了受争议的新安全模型以外的部份，在安全方面依然沿袭了 SNMPv1 的团体名认证方式。SNMPv2c 也被非正式的称为 SNMP 的第 1.5 版。

SNMPv2c 在兼容 SNMPv1 的同时，对 SNMPv1 的功能进行了扩充，主要说明如下。

(1) SNMPv2c 提供了对分布式网络管理的支持。在 SNMPv2c 中，网络中可以分层次地存在多个 SNMP 管理者，其中中间管理者同时承担着 SNMP 管理者和 SNMP 代理两种角色，一方面它以 SNMP 代理的身份接受上一级 SNMP 管理者的管理，另一方面又作为 SNMP 管理者对下属的 SNMP 代理进行管理。分布式管理有效的减轻了顶级 SNMP 管理者的负担，分散了 SNMP 管理流量，适用于大中型网络的管理。

(2) SNMPv2c 中增加了两种新的 PDU。

① Get-Bulk-Request：Get-Bulk-Request 是对 Get-Next-Request 的改进，它可以使 SNMP 管理者高效率地从 SNMP 代理处获得大量被管理对象的数据。Get-Bulk-Request 通过设定 Non repeaters 和 Max repetitions 参数，允许 SNMP 管理者请求得到在给定的条件下尽可能多的应答，从而尽量减少查询大量信息时所进行的协议交换次数。

② Inform-Requset：Inform-Requset 用于在 SNMP 管理者之间进行通信。它被认为是低级别 SNMP 管理者向自己的上级 SNMP 管理者发送的 Trap 报文。从广义上讲 SNMP 协议的 Trap 可以分为 Trap 和 Inform-Requset 两种，区别在于 SNMP 管理者在收到一条 Trap 通知后无需回复任何确认信息；而在收到一条 Inform-Requset 通知后，需要回复 Reponse 作为确认信息。

(3) SNMPv2c 改进了 SNMPv1 的管理信息结构 (Structure of Management

Information,SMI)。SNMPv2c 定义扩充了对象类型宏,增强了对象表达能力,扩展了数据类型。SMI 的具体概念在下一节进行介绍。

目前,提及 SNMPv2 一般都是指 SNMPv2c。

出于对 SNMP 通信安全性的考虑,在 2004 年发布了 SNMPv3,SNMPv3 主要增强了 SNMP 协议的安全性,它采用基于用户的安全模型(User-Based Security Model,USM)和基于视图的访问控制模型(View-based Access Control Model,VACM)技术来实现数据的机密性以及用户的访问合法性等安全策略。

(1) USM:USM 引入了用户名和组的概念,可以设置认证和加密功能。认证用于验证报文发送方的合法性,避免非法用户的访问;加密用于对 SNMP 管理者和 SNMP 代理之间传输的报文,以免被窃听。通过有无认证和有无加密等功能的组合,可以为 SNMP 管理者和 SNMP 代理之间的通信提供更高的安全性。

(2) VACM:VACM 技术定义了组、安全等级、上下文、MIB 视图、访问策略等 5 个元素,这些元素同时决定用户是否具有访问权限,只有具有了访问权限的用户才能管理操作对象。在同一个 SNMP 实体上可以定义不同的组,组与 MIB 视图绑定,组内又可以定义多个用户。当使用某个用户名进行访问的时候,只能访问对应的 MIB 视图定义的对象,从而避免了用户的越权非法访问。

7.3.2 MIB 与 RMON

1. MIB

作为被管理对象的信息集合,为确保 MIB 中各个被管理对象在语义和语法上的明确和唯一,在 SNMP 协议中使用管理信息结构(Structure of Management Information,SMI)语言对被管理对象的对象模型、数据类型、命名方法以及写入修改规则等进行了定义。在 SMI 中,使用抽象语法符号(Abstract Syntax Notation One,ASNO)对被管理对象进行描述,在该描述中,MIB 以树形结构进行存储,如图 7-3 所示。

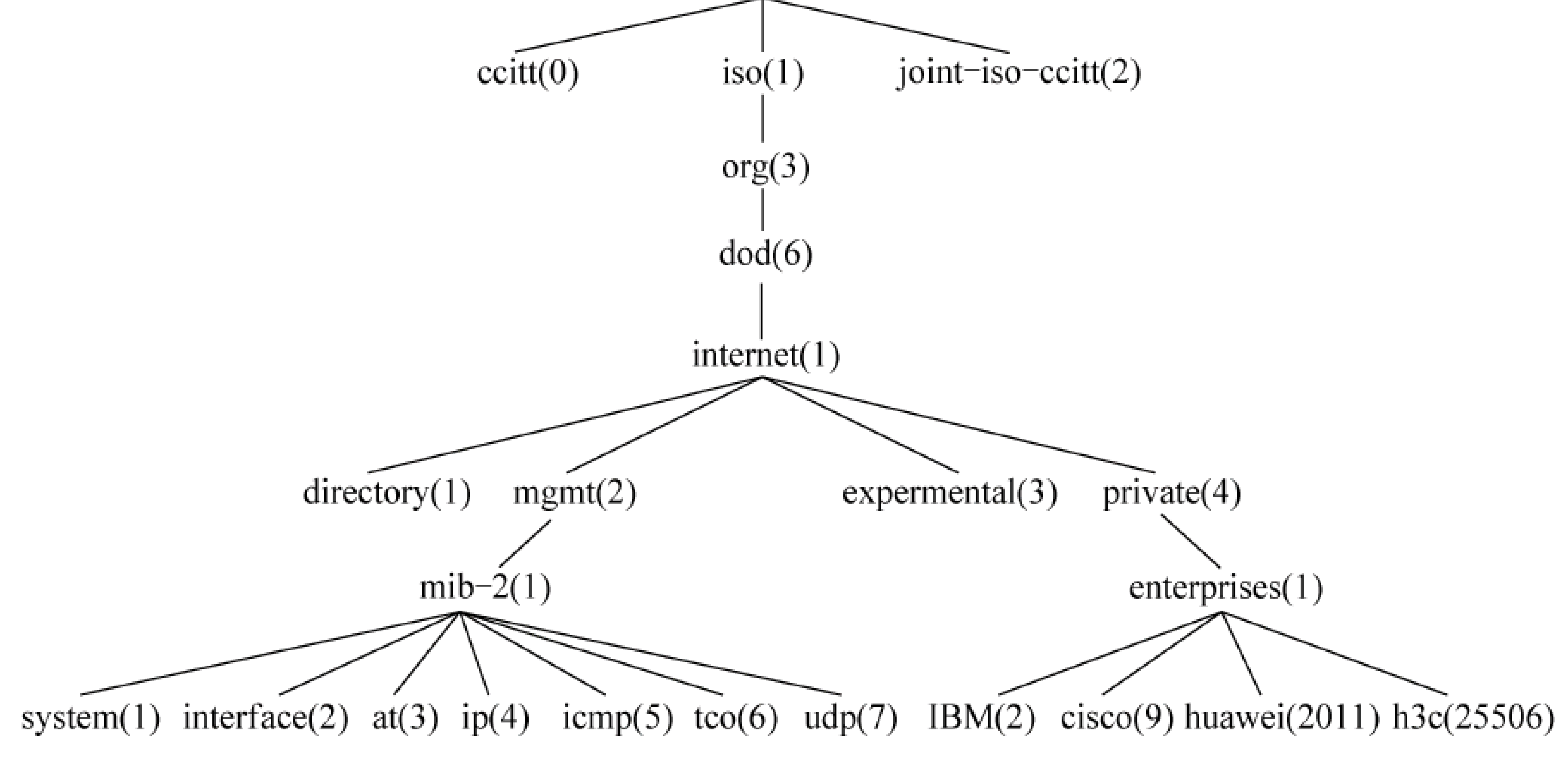


图 7-3 MIB 树形结构示意图

在 MIB 的树形结构中,树的叶节点表示被管理对象,每一个被管理对象或子树都可以用从根开始的一条路径来唯一地识别,这条用数字串来表示的路径称为被管理对象或

子树的对象标识符(Object Identifier,OID)。例如,以 mib-2 为根节点的子树的 OID 为{1.3.6.1.2.1},也可以表示为{mgmt.1},即 mib-2 为 mgmt 的第一棵子树。

在 MIB 树中,顶级对象有 3 个,分别是 ITU-T、ISO 和这两个组织的联合体;在 ISO 下面有 4 个节点,其中 org 是被标识的组织;在 org 下存在一个美国国防部(Department of Defense)的节点 dod;在 dod 下存在节点 internet,用到的被管理对象均在 internet 之下;在 internet 下的 mgmt 中存在一个 mib-2 的节点,早期该节点的名称为 mib,在管理信息库升级为第 2 版后,该节点的名称被改为 mib-2,目前在 mib-2 下存在四十余个节点。在 internet 下的 private 中存在节点 enterprises,该节点之下供设备厂商和企业申请属于自己的节点,在申请到节点后,各个厂商就可以定义自己私有的被管理对象,使之能被 SNMP 协议管理。目前在 enterprises 下存在数千个节点,例如 IBM 为 2、Cisco 为 9、Microsoft 为 311、华为为 2011、H3C 为 25506。

在 MIB 树的叶节点中存放有访问函数的指针,在 SNMP 代理访问某个被管理对象时,首先会根据该对象的 OID 找到其对应的叶节点,然后调用该叶节点对应的函数来获得相应被管理对象的管理变量,从而实现相应的操作。在 SNMP 的报文中,Variable bindings 字段中包含了 SNMP 访问的被管理对象 OID 以及相应的变量值信息,如图 7-4 所示。

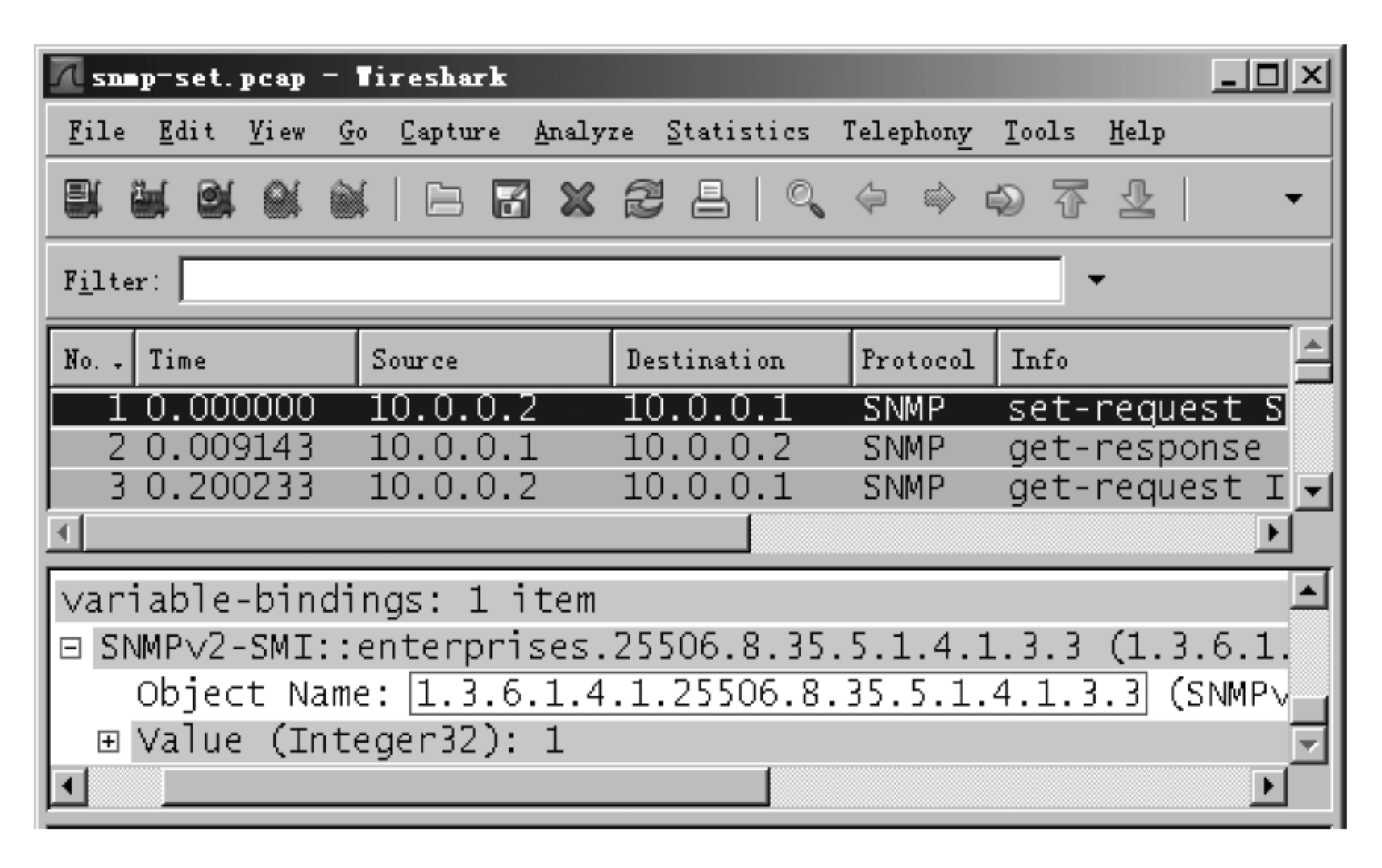


图 7-4　SNMP 报文中的 OID

2. RMON

在 SNMP 协议中,SNMP 管理者通过轮询来采集被管理设备的数据信息,轮询会产生大量的网络管理报文,从而可能导致网络的拥塞,甚至是网管工作站的崩溃,为此引入了远程网络监视(Remote Monitoring,RMON)技术。RMON 实际上是由 IETF 定义的一种 MIB,它通过对 SNMP 的 MIB-2 进行扩展,使 SNMP 管理者可以将一个网段当做一个整体来监视,从而减少 SNMP 管理者与 SNMP 代理之间的网络管理流量、减轻网关工

作站的负担,使SNMP可以更有效地管理远程网络设备。

RMON定义的MIB包含9个信息组,分别是统计组、历史组、告警组、主机组、最高N台主机组、矩阵组、过滤组、包捕获组和事件组,这9个组分别提供不同的统计数据和分析数据来满足网络管理和监控的实际需要。

作为与SNMP框架完全兼容的技术,RMON同样分为网管工作站(Network Management Station,NMS)和网管代理两部分。NMS收集数据的方法有两种:

(1) 通过专门的RMON Probe探测仪收集数据。RMON代理运行于专门的RMON探测仪上,NMS直接从RMON探测仪获取网络管理信息并控制网络资源。这种方式可以获取RMON MIB的全部信息,但实现成本较高。

(2) 从被管理的网络设备上收集数据。将RMON代理直接植入网络设备,使网络设备具备RMON探测仪的功能。NMS利用SNMP的基本命令与运行于网络设备上的RMON代理之间进行数据信息交换,收集网络管理信息。受到设备资源的限制,该方法一般无法获取RMON MIB的所有数据,大多数情况下只收集统计组、历史组、告警组和事件组4个组的信息。

在实际应用中,一般都采用第2种方法来实现,即在网络设备上内置支持RMON功能的SNMP代理进程。NMS通过与SNMP代理交互就可以获得被管理设备的接口或端口相连网段上的整体流量、错误统计和性能统计等信息,从而实现对网络的远程管理。

7.4 网络管理的配置

作为网络管理代理端,当前的网络设备一般都能提供对SNMPv1、SNMPv2c和SNMPv3三个版本SNMP协议的支持,但早期的网络设备可能无法支持SNMPv3,因此在这里以SNMPv1和SNMPv2c的配置方法为例对网络管理的配置进行介绍。

7.4.1 H3C设备的配置

在H3C网络设备上,SNMP协议配置涉及的基本命令如下。

(1) 启动SNMP代理服务。

```
[H3C]snmp-agent
```

在默认情况下,SNMP代理服务处于关闭状态,必须通过snmp-agent命令将其启动。

(2) 设置SNMP的系统信息。

```
[H3C]snmp-agent sys-info {contact sys-contact | location sys-location |version {v1|v2c|v3|all}}
```

默认情况下,系统维护联系信息为"R&D Hangzhou, Hangzhou H3C Technologies Co., Ltd.",在设备发生故障时,维护人员可以根据系统维护联系信息及时与设备生产厂商取得联系;物理位置信息为"Hangzhou, China";版本信息为v3。

(3) 设置SNMP的团体名。

```
[H3C]snmp-agent community {read|write} community-name
```

一般建议配置的只读团体名和读写团体名不要相同,并且团体名应具备足够的复杂

度，应尽量避免使用有意义的字符串。

(4) 设置本地引擎 ID。

```
[H3C]snmp-agent local-engineid engineid
```

默认情况下，本地引擎 ID 为设备生产厂商的“企业号＋设备信息”，例如：800063A2033CE5A61354B6。

(5) 启动 SNMP 的 Trap 功能，使网络设备可以向网管工作站发送 Trap 信息。

```
[H3C]snmp-agent trap enable
```

(6) 设置 Trap 的目标主机地址，即网管工作站的地址。

```
[H3C]snmp-agent target-host trap address udp-domain ip-address [udp-port port-number] params
securityname security-string
```

其中，参数 *ip-address* 为网管工作站的地址，即指定网络设备向谁发送 Trap 信息；*port-number* 默认为 162；*security-string* 要和之前配置的只读团体名相同。

SNMPv3 的配置与 SNMPv1 和 SNMPv2c 的配置存在较大的差异，在 SNMPv3 的配置中需要配置组和用户等信息。为保持配置命令的一致性，SNMPv1 和 SNMPv2c 也可以采用与 SNMPv3 相一致的命令形式进行配置。如果采用 SNMPv3 的命令形式进行 SNMPv1 和 SNMPv2c 的配置，则配置的用户名即为 SNMPv1 和 SNMPv2c 的团体名。

以上所介绍的是 SNMP 代理端的配置，在配置完代理端后，还需要对 SNMP 管理者即网管工作站进行相应的配置，才能对网络进行管理。所谓的网管工作站实际上就是指运行网络管理系统的主机。目前常用的网络管理系统软件种类繁多，能够提供的功能和系统规模相差很大，既有能够提供五大网络管理功能的标准网络管理平台，例如，HP 公司的 OpenView、IBM 公司的 NetView；又有只能提供部分网络管理功能的软件，例如，进行网络安全审查的 Nessus、进行网络性能监控的 PRTG 等。在这里我们使用的网络管理软件为 H3C 公司的智能管理中心(Intelligent Management Center，iMC)，作为 H3C 推出的下一代业务智能管理产品，iMC 以全开放、组件化的架构原型，以统一的风格向用户提供与网络相关的各类管理、控制和监控等功能。

假设存在如图 7-5 所示的网络，其中网络的联通性配置已经完成，要求进行 SNMP 的配置，使其可以被网管工作站 NMS 上的 iMC 管理。其中只读团体名为 public，读写团体名为 private。

4 台网络设备上的 SNMP 配置完全相同，其中 RTA 上的配置命令如下：

```
[RTA]snmp-agent
[RTA]snmp-agent sys-info version all
[RTA]snmp-agent community read public
[RTA]snmp-agent community write private
[RTA]snmp-agent trap enable
[RTA]snmp-agent target-host trap address udp-domain 192.168.1.3 params securityname public
```

配置完成后，使用 display current-configuration 命令查看 SNMP 的配置情况如下：

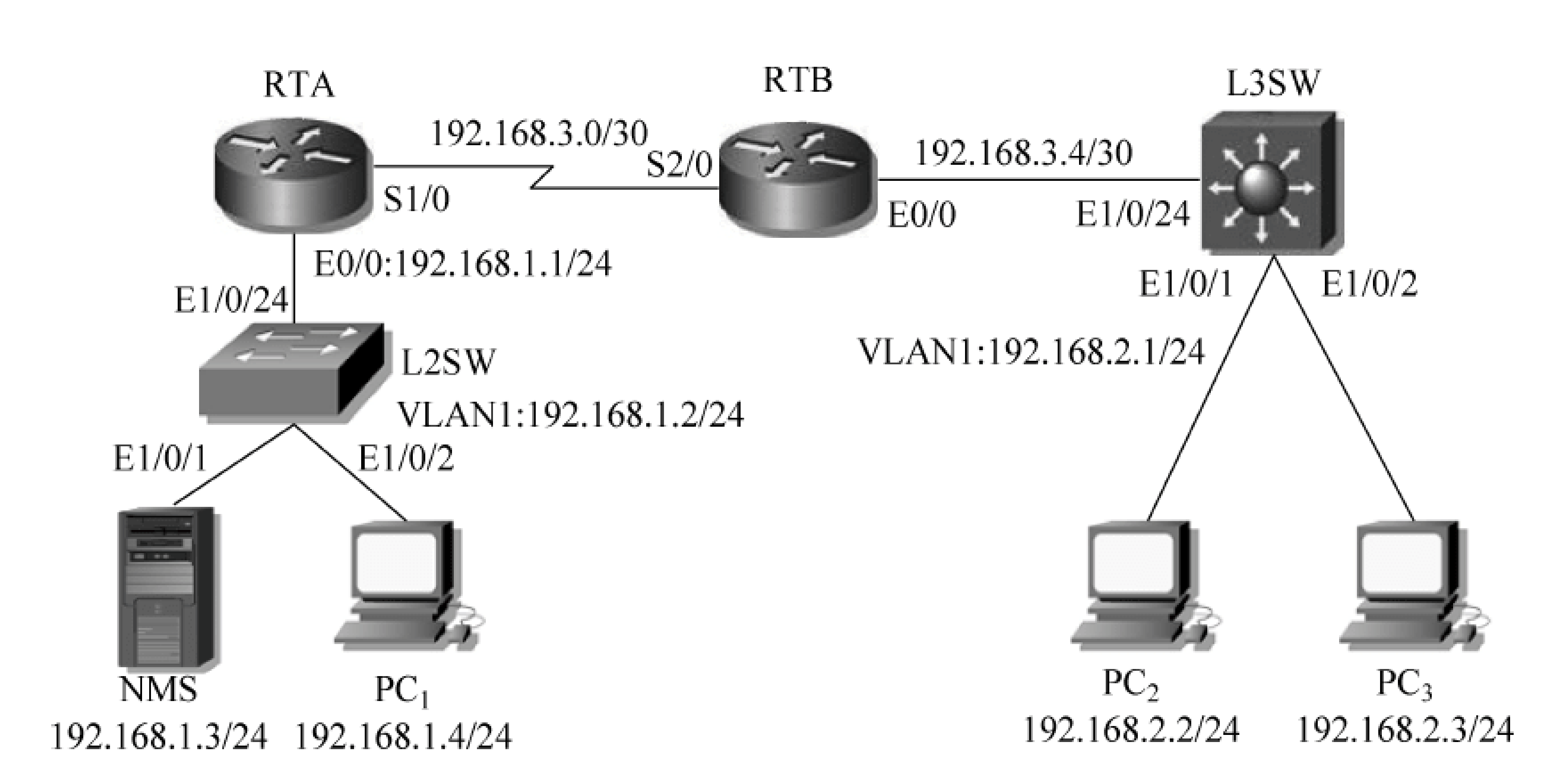


图 7-5　网络管理配置

```
[RTA]display current-configuration | include snmp
snmp-agent
snmp-agent local-engineid 800063A2033CE5A61354B6
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 192.168.1.3 params securityname public
```

RTB、L2SW 和 L3SW 上的配置略。

网络设备即 SNMP 的代理端配置完成后，在 NMS 上启动 iMC 对网络进行管理。关于 iMC 的具体安装过程详见附录 D，在这里只对其应用进行介绍。在 NMS 上选择“开始—程序—H3C 智能管理中心—H3C 部署监控代理”，弹出“智能部署监控代理”界面，如图 7-6 所示。



图 7-6　智能部署监控代理

在“智能部署监控代理”界面单击“启动 iMC”来启动 iMC 服务，这个过程可能需要花费数分钟的时间。在 iMC 启动后，单击“进程”选项卡可以看到所有进程均已处在“已经启动”的状态。

iMC 启动后，在 NMS 上打开 IE 浏览器，输入地址“http://localhost:8080/imc”即可进入 iMC 的登录页面。iMC 默认的用户名和密码均为 admin，输入用户名和密码登录进入 iMC 的首页，如图 7-7 所示。

此时，iMC 中不包含任何的网络设备，因此首先需要增加被管理的网络设备。在 iMC 中增加设备有两种方法：一种方法是手动增加，通过这种方法可以向 iMC 中增加指定的一台设备，一般用于在已存在的被管理网络中增加一台新的网络设备；另一种方法



图 7-7　iMC 首页

是自动发现，是由 iMC 自动去查询发现网络中存在的可管理设备，一般用于初次使用 iMC 时快速完成网络设备的批量增加。在这里使用自动发现功能来批量增加网络设备。

在首页的左侧“功能导航”栏中选择“自动发现”，或者在“资源”页签下的“资源管理”栏中选择“自动发现”，进入“自动发现（简易）”界面，如图 7-8 所示。

自动发现(简易)　切换到高级模式　设置缺省监视指标

网段设置(必须)

开始IP

结束IP

* 已设置的网段地址

增加

删除

设备分组

SNMP & Telnet 参数设置

* SNMP读团体字

* SNMP写团体字

* Telnet认证模式　无用户名 +无密码

定时发现设置

* 定时发现方式　从不

仅保存设置　自动发现

图 7-8　“自动发现（简易）”界面

在“自动发现(简易)”界面的右上角单击“切换到高级模式”,可以切换到高级自动发现界面,如图 7-9 所示。



图 7-9　高级自动发现界面

在高级自动发现界面中可以根据具体的应用需求选择不同的发现方式,在了解网络中网段规划信息的情况下,推荐使用“以网段方式发现”,即“自动发现(简易)”界面中使用的方式。在图 7-8 中增加需要进行发现的网段,并设置 SNMP 的团体名,如图 7-10 所示。

自动发现(简易)　切换到高级模式　设置缺省监视指标
网段设置(必须)
开始IP
结束IP　增加
* 已设置的网段地址　192.168.1.1-192.168.1.4　192.168.2.1-192.168.2.3　192.168.3.1-192.168.3.6　删除
设备分组
SNMP & Telnet 参数设置
* SNMP读团体字　public
* SNMP写团体字　private
* Telnet认证模式　无用户名 +无密码
定时发现设置
* 定时发现方式　从不
仅保存设置　自动发现

图 7-10　自动发现参数配置

在图 7-10 中单击“自动发现”按钮开始自动发现过程。iMC 自动发现完成后,显示结果如图 7-11 所示。

从图 7-11 所显示的自动发现结果可以看出,iMC 共发现了 8 个设备,其中 SNMP 设备 4 个,分别是路由器 RTA 和 RTB、交换机 L2SW 和 L3SW,ICMP 设备 4 个,分别是 PC_1、PC_2、PC_3 和 NMS。在图 7-11 中单击“查看报表”可以查看在自动发现过程中出现的问题,并可将报表导出为 RPT、PDF、WORD 或 EXCEL 格式。

在“资源”标签下单击“网络拓扑视图”进入“拓扑”页面,在“拓扑”页面下双击“我的网络拓扑”,可以查看 iMC 发现的网络拓扑,如图 7-12 所示。

运行自动发现

自动发现结束。共发现8个设备，其中：SNMP设备4个，ICMP设备4个。新增加8个设备。

查看报表　接入设备与核心设备配置

时间	新发现的设备	结果
2012-05-07 19:38:26	自动发现结束。	共发现8个设备，其中：SNMP设备4个，ICMP设备4个。新增加8个设备。
2012-05-07 19:38:25	PC1(192.168.1.4)	增加设备 “PC1(192.168.1.4)”成功。
2012-05-07 19:38:19	L2SW(192.168.1.2)	增加设备 “L2SW(192.168.1.2)”成功。
2012-05-07 19:37:57	PC2(192.168.2.2)	增加设备 “PC2(192.168.2.2)”成功。
2012-05-07 19:37:57	PC3(192.168.2.3)	增加设备 “PC3(192.168.2.3)”成功。
2012-05-07 19:37:42	NMS(192.168.1.3)	增加设备 “NMS(192.168.1.3)”成功。
2012-05-07 19:37:38	L3SW(192.168.2.1)	增加设备 “L3SW(192.168.2.1)”成功。
2012-05-07 19:37:34	RTB(192.168.3.2)	增加设备 “RTB(192.168.3.2)”成功。
2012-05-07 19:37:30	RTA(192.168.3.1)	增加设备 “RTA(192.168.3.1)”成功。
2012-05-07 19:36:57	自动发现开始。	自动发现开始。

图 7-11　自动发现结果

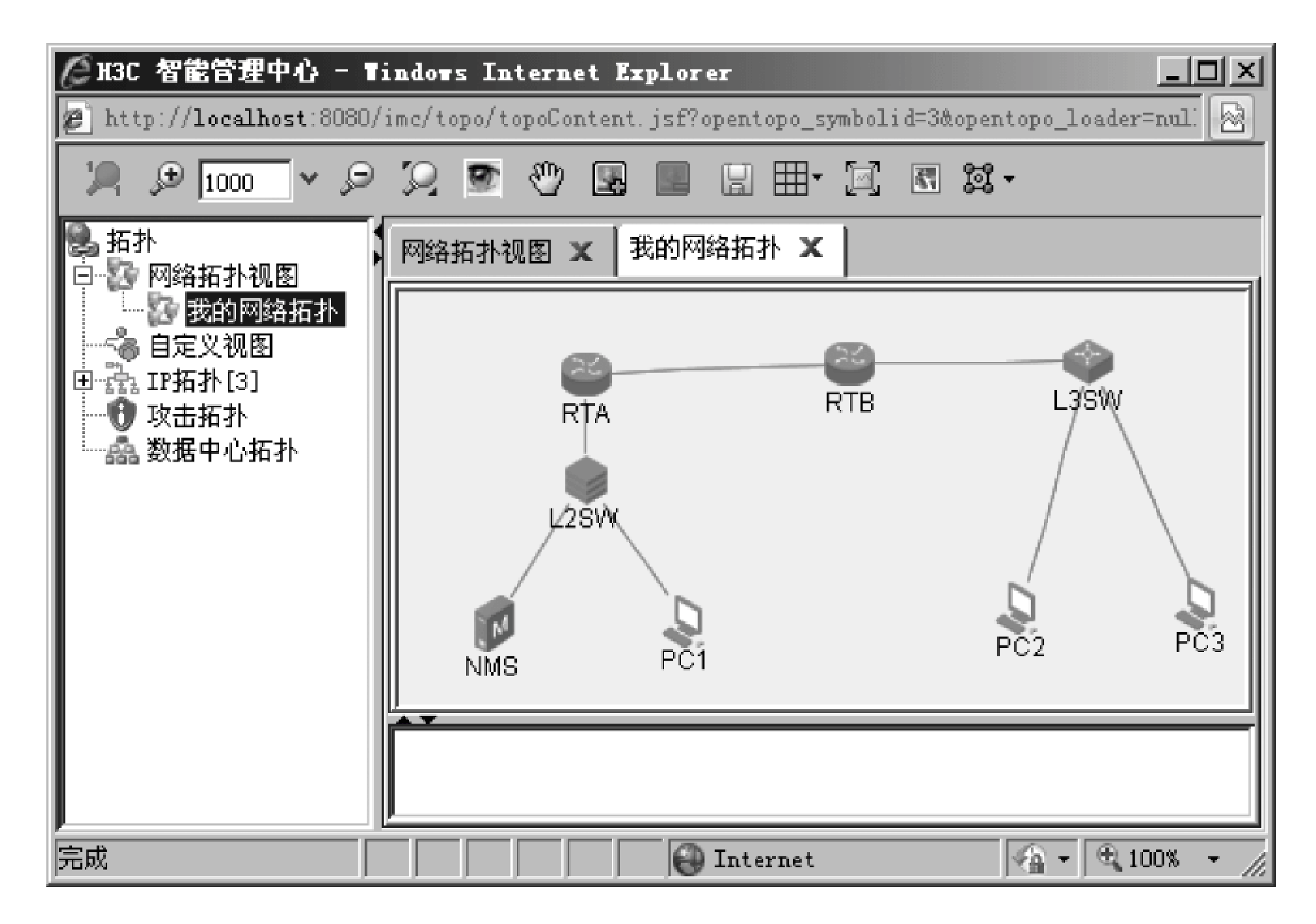


图 7-12　iMC 网络拓扑图

在有些时候，iMC 发现的网络拓扑可能不完整，如缺少某些链路，这时候可以对缺少的链路进行添加。添加链路的方法如下：按住 Ctrl 键，选择需要添加链路的两台设备，在设备上右击，并在弹出的菜单中选择“同步”，同步成功后，在空白处右击，并在弹出的快捷菜单中选择“重新加载”，则 iMC 会自动添加被选中的两台设备之间的链路。

在网络拓扑图中，用鼠标单击任何一台网络设备或者链路，就会显示该设备或链路的基本信息，如果双击某一条链路或者右击某一条链路并在弹出的菜单中选择“链路信息”，则会显示该链路的基本信息和链路两端接口的详细信息。路由器 RTB 和交换机 L3SW

之间的链路的基本信息和左接口的详细信息如图 7-13 和图 7-14 所示。

链路信息

基本信息　左接口　右接口

链路名称	L3SW - RTB
连接状态	正常
连接类型	Ethernet CSMACD
左节点	L3SW
左接口描述	Ethernet1/0/24
右节点	RTB
右接口描述	Ethernet0/0

确定

图 7-13　RTB-L3SW 链路基本信息

链路信息

基本信息　左接口　右接口

接口描述	Ethernet1/0/24	别名	Ethernet1/0/24 Interface
管理状态	Up	接口类型	ethernetCsmacd
操作状态	Up	IP地址	192.168.3.6
最大传输单元	1500	IP地址掩码	255.255.255.252
接口速度	100M	物理地址	3c:e5:a6:09:e1:b1
上次改变状态时间	2012-05-07 17:29:38	最近一次刷新时间	2012-05-07 19:37:38

查看MP接口　查看接口POE

确定

图 7-14　RTB-L3SW 链路左接口信息

在网络拓扑图中，右击某一台设备并在弹出的菜单中选择“打开设备面板”，则可以将该设备的物理面板情况展示出来。交换机 L3SW 的面板情况如图 7-15 所示。



图 7-15　交换机 L3SW 面板

在图 7-15 中，接口的颜色直观地反应当前接口所处的状态，如果接口颜色为绿色，则表示接口处于 UP 状态；如果接口颜色为红色，则表示接口处于 DOWN 状态；如果接口

颜色为蓝色，则表示接口的状态为 Unknown。在接口上右击，并在弹出的快捷菜单中选择“端口管理”，可以对接口的状态、速率以及工作方式等参数进行设置和管理。

单击“首页”标签，返回首页，可以看到当前 iMC 管理的设备视图快照和设备状态快照，如图 7-16 所示。



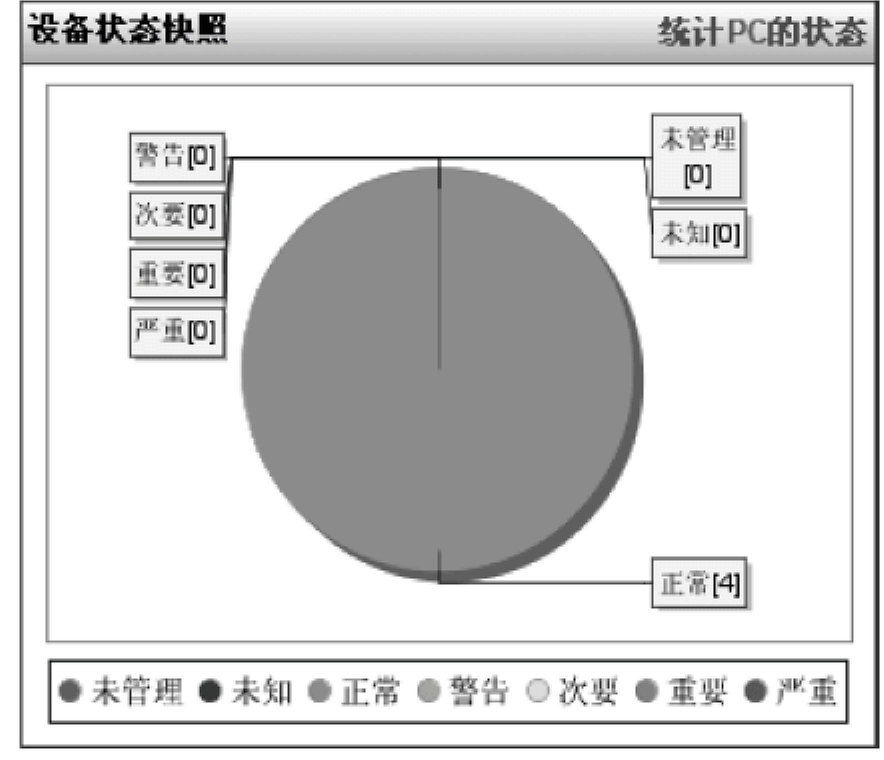


图 7-16　设备快照

在“设备视图快照”栏中单击相应的设备，进入“设备信息列表”界面，路由器的“设备信息列表”界面如图 7-17 所示。

设备信息列表 - 全部

删除 | 管理 | 取消管理 | 同步 | 刷新 | 更多操作...

共有2条记录，当前第1-2，第 1/1 页。　　每页显示：8 15 [50] 100 200

	状态	设备标签▲	在线用户	型号	IP地址	接口列表	操作
□	正常	RTA(192.168.3.1)		H3C MSR20-40	192.168.3.1	接口列表	
□	重要	RTB(192.168.3.2)		H3C MSR20-40	192.168.3.2	接口列表	

图 7-17　路由器的“设备信息列表”

从图 7-17 中可以看到，路由器 RTB 的状态为“重要”，这说明路由器 RTB 存在告警级别为“重要”的告警。在图 7-17 中单击路由器 RTB 的设备标签，进入路由器 RTB 的具体管理界面，在该界面下可以看到路由器 RTB 的设备详细信息、服务信息、告警信息、性能监视信息以及配置管理信息。其中性能监视信息如图 7-18 所示。

性能监视　　更详细数据

监视指标	监视值
CPU最近一小时利用率平均值-[实体:Module Level1]	1.000%
内存最近一小时利用率平均值-[实体:Module Level1]	52.091%
设备今天不可达比例平均值	0.000%
设备最近一小时响应时间平均值	153.667 ms

图 7-18　RTB 的性能监视信息

在图 7-18 中单击“更详细数据”或者在路由器 RTB 的具体管理界面右侧的“性能监视”栏中单击“查看性能数据”，可以查看路由器 RTB 在某一时间段中的内存利用率、设备

不可达性比例、CPU利用率以及设备响应时间等性能监控数据信息。其中路由器RTB最近一小时的设备响应时间折线图如图7-19所示。

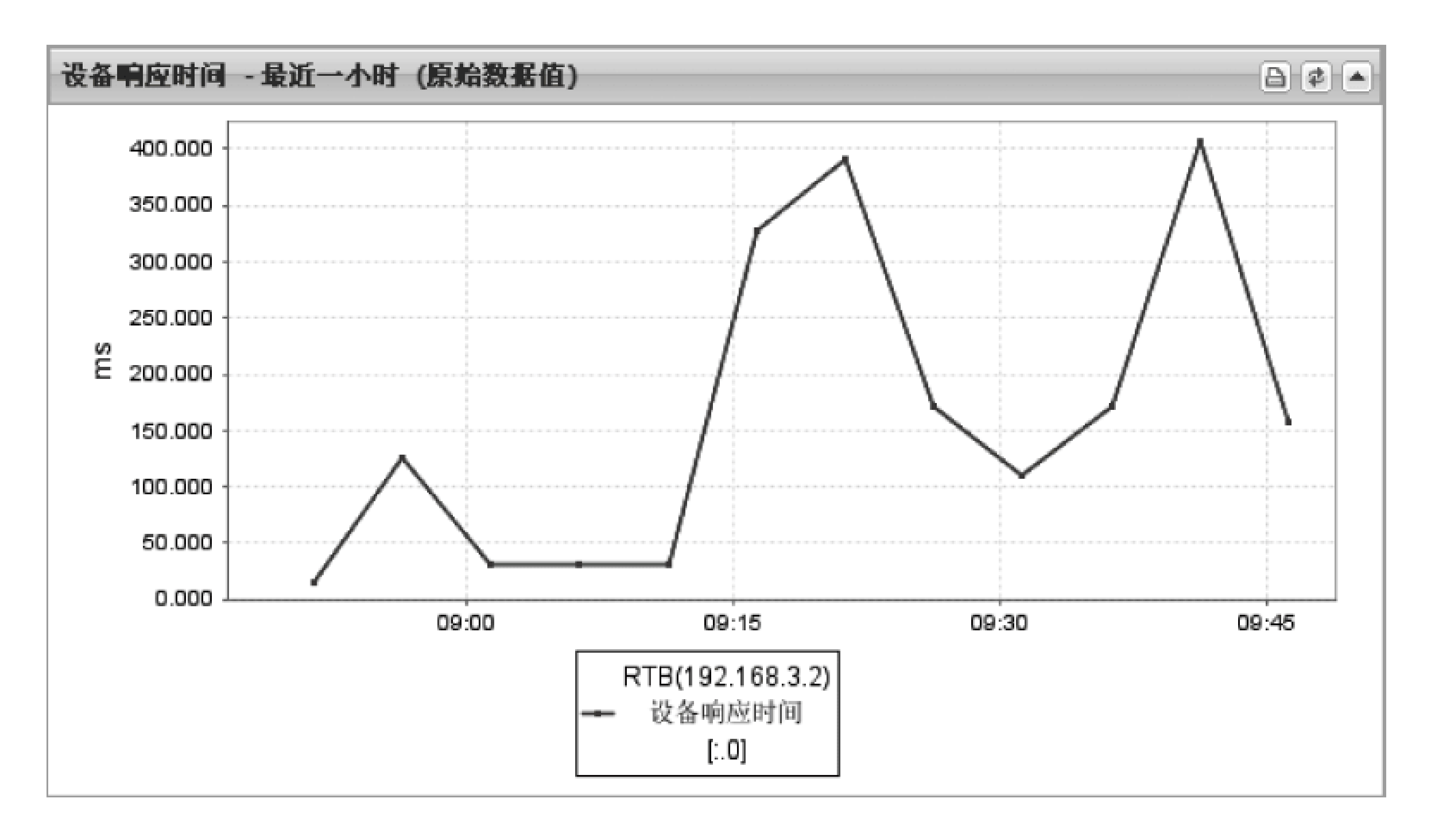


图7-19 路由器RTB最近一小时的设备响应时间

在“资源”页签左下角的“性能管理”栏中单击“TopN”可以查看某一时间段中网络中的各个设备的内存利用率、设备不可达性比例、CPU利用率以及设备响应时间的统计信息排序列表。其中最近一小时的内存利用率的TopN如图7-20所示。TopN是基于RMON技术实现的。

内存利用率的TopN - 最近一小时

设备名称	实例	数据
RTB(192.168.3.2)	[实体:Module Level1]	52.000%
RTA(192.168.3.1)	[实体:Module Level1]	52.000%
L3SW(192.168.3.6)	[实体:virtual board]	47.000%
L2SW(192.168.1.2)	[内存:.65536]	31.330%

图7-20 最近一小时的内存利用率TopN

在默认情况下，iMC只对内存利用率、设备不可达性比例、CPU利用率以及设备响应时间共4项指标进行监视。如果需要增加性能监视项，可以在“资源”标签左下角的“性能管理”栏中单击“监视设置”进行配置。

假设需要为路由器RTB增加对“接口输入带宽利用率”指标的监控。具体操作过程为：在“监视设置”界面下单击“增加监视”按钮，进入“增加监视”界面；在“增加监视”界面下单击“选择设备”，弹出“设备选择”对话框；在“设备选择”对话框中选择设备RTB，将其置入已选择设备中，并单击“确定”按钮返回“增加监视”界面；在“增加监视”界面下选中设备RTB，并单击“选择指标”按钮，弹出“选择指标”对话框；在“选择指标”对话框中找到“系统—接口统计—接口输入带宽利用率”指标项并选中，单击“确定”按钮返回“增加监视”界面；在“增加监视”界面下单击“确定”完成性能监视指标的增加。增加完成后显示操作结果如图7-21所示。

此时,查看路由器 RTB 的性能数据可以看到增加了关于“接口输入带宽利用率”的监控数据信息。

iMC 还有一部分很重要的内容就是告警管理,在 iMC 页面的下方存在告警信息栏,如图 7-22 所示。

操作结果

共有1条记录。

设备名称	设备型号	设备IP	操作结果
RTB(192.168.3.2)	H3C MSR20-40	192.168.3.2	成功

图 7-21　增加监视操作结果

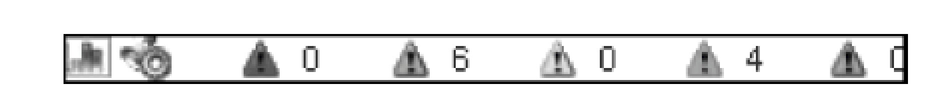


图 7-22　告警信息栏

在“告警信息栏”中,最左侧的图标为“分类告警板”,单击该图标可以打开“分类告警板”界面,来显示当前各种未恢复告警的统计情况;第二个图标为“告警声音设置”,单击该图标可以设置各种不同级别告警的告警声音提示;剩下的五个图标,从左至右依次为紧急告警、重要告警、次要告警、警告告警和通知告警,图标后面的数字为该类型告警中未恢复的告警数量,单击图标后面的数字即可进入相应的告警列表界面。

用鼠标单击“告警”标签,进入“告警”界面;在“告警”界面中左侧的“告警浏览”中可以选择查看实时告警、当前告警、全部告警以及存在故障的设备。其中“全部告警”界面如图 7-23 所示。



	级别	告警来源	类型	告警信息	恢复状态	确认状态	告警时间	恢复时间	持续时间
	重要	RTB (192.168.3.2)	iMC	性能任务(设备响应时间)中设备(RTB)实例([:.0])处于阈值区域:>=100,当前值为468。	admin	admin	2012-05-08 11:56:19	2012-05-08 12:02:17	5分钟 58秒
	次要	RTB (192.168.3.2)	iMC	性能任务(设备响应时间)中设备(RTB)实例([:.0])处于告警阈值区域:>=50,当前值为250。	未恢复	未确认	2012-05-08 11:51:19		12分钟 10秒
	通知	L2SW (192.168.1.2)	Trap	连接设备L2SW(192.168.1.2)的接口Ethernet1/0/2的状态UP。	$SYSTEM	未确认	2012-05-08 11:37:56	2012-05-08 11:37:56	0秒
	重要	L2SW (192.168.1.2)	Trap	连接设备L2SW(192.168.1.2)的接口Ethernet1/0/2的状态DOWN。	$SYSTEM	未确认	2012-05-08 11:37:52	2012-05-08 11:37:56	4秒
	通知	L3SW (192.168.3.6)	iMC	性能任务(设备响应时间)中设备(L3SW)实例([:.0])恢复正常,当前值为32。	$SYSTEM	未确认	2012-05-08 10:46:19	2012-05-08 10:46:19	0秒

图 7-23　全部告警列表信息

在图 7-23 的上半部分可以通过设置告警时间、告警级别以及告警类型等条件参数来查询特定的告警信息。选中告警记录并单击“恢复”或“确认”按钮可以对相应的告警记录信息进行恢复或确认。单击某一条告警记录中的“告警信息”字段可以查看该条告警记录的详细信息,在图 7-23 中单击第 4 条告警记录的“告警信息”字段显示的结果如图 7-24 所示。

告警详细信息

名称	链路DOWN
级别	重要
OID	1.3.6.1.6.3.1.1.5.2.0
告警时间	2012-05-08 11:37:52
告警来源	L2SW(192.168.1.2) 更多告警...
类型	Trap
告警分类	接口\链路状态告警
恢复状态	$SYSTEM
恢复时间	2012-05-08 11:37:56
确认状态	未确认
详细信息	连接设备L2SW(192.168.1.2)的接口Ethernet1/0/2的状态DOWN。
告警原因	链路状态由UP变为DOWN，可能的原因：1、用户disable接口；2、连接该接口的网线被拔掉或者损坏；3、接口配置中，接口的IP被删除；4、链路中对端接口故障。
修复建议	1、检查该接口的配置是否为disable，如果是，请使能该接口；2、检查连接该接口的网线是否松动或者损坏；3、检查设备配置，确定该接口是否有正确的IP地址；4、检查对端接口是否故障。
维护经验	
告警参数	

参数名称	参数值
*Interface Index	4227634
Interface Description	Ethernet1/0/2
Interface Admin Status	1
Interface Operate Status	2

图 7-24　告警详细信息

对于经常出现的一些告警信息,可以为其编辑维护经验,以备再次遇到相同的问题时可以根据已有的维护经验对其进行处理。在“告警详细信息”界面的右侧“动作”栏中单击“编辑维护经验”弹出“编辑维护经验”对话框,如图 7-25 所示。



图 7-25　编辑维护经验

在图 7-25 所示的对话框中输入维护经验，单击“确定”按钮，输入的维护经验就会显示在图 7-24 中的“维护经验”字段部分。

在 iMC 上可以通过打开被管理网络设备的 Web 界面或者 Telnet/SSH 到网络设备上对设备进行配置管理。在“设备信息列表”界面中单击相应网络设备“操作”字段下的“操作”图标，弹出操作菜单，如图 7-26 所示。



图 7-26　设备操作菜单

从图 7-26 中可以看到，可以通过 ping 命令或者 TraceRoute 命令测试到达相关设备的联通性；可以通过 Web、Telnet 或者 SSH 的方式对网络设备进行配置管理。当然，可以 Telnet 或者 SSH 的前提是网络设备上已经开启了相应的服务并且在 iMC 上配置了登录使用的用户名、密码等参数。在 iMC 上可以通过配置相关的模板来设置登录设备信息，在 iMC 中单击“系统管理”页签，进入“系统管理”界面，在该界面下的“资源管理”栏如图 7-27 所示。

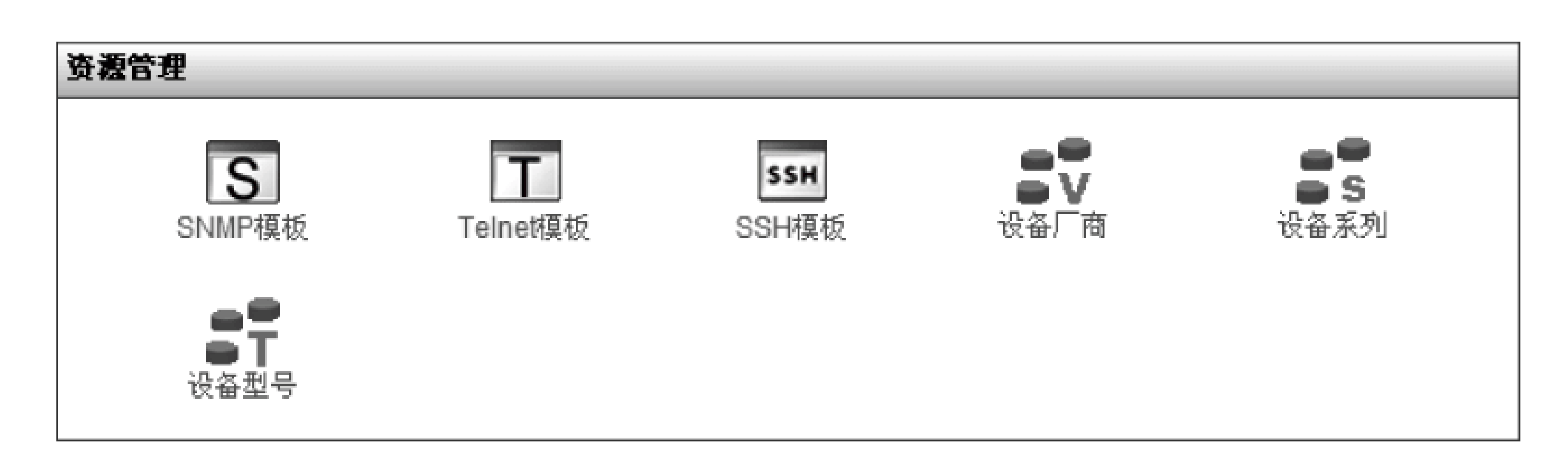


图 7-27　资源管理栏

从图 7-27 中可以看到，可以对 SNMP 模板、Telnet 模板以及 SSH 模板进行配置。在此以 Telnet 模板为例进行介绍。单击“Telnet 模板”进入“Telnet 模板列表”界面，如图 7-28 所示。

在图 7-28 中可以单击已有模板中的“修改 Telnet 模板”图标对已有的模板进行修改，也可以单击“增加”按钮增加新的 Telnet 模板。“增加 Telnet 模板”界面如图 7-29 所示。



Telnet模板列表

增加 刷新

共有1条记录。

模板名称	认证模式	超时时间(秒)	修改	删除
default	无用户名 +无密码	4		

图 7-28 Telnet 模板列表

增加Telnet模板

* 模板名称	
* 认证模式	用户名 +密码
* 用户名	
密码	
* 超时时间(1-60秒)	4

确定 取消

图 7-29 增加 Telnet 模板

增加了新的 Telnet 模板后,在设备的具体管理界面右侧的“配置”栏中单击“修改 Telnet 参数”弹出“Telnet 参数设置”对话框,如图 7-30 所示。

http://localhost:8080/imc/res/paratemplate/telnet/selectContent.jsf - Windows Interne...

http://localhost:8080/imc/res/paratemplate/telnet/selectContent.jsf

Telnet参数设置

手工编辑Telnet参数 从已有的Telnet参数模板中选取 刷新

选择	模板名称	认证模式	用户名	超时时间(秒)
○	default	无用户名 +无密码		4
⊙	aaa	用户名 +密码	abc	4

确定 取消

Internet 100%

图 7-30 Telnet 参数设置

在图 7-30 中选择合适的 Telnet 模板,或者手工编辑 Telnet 参数,使其符合网络设备的登录认证要求。然后在图 7-26 弹出的菜单中单击“Telnet 设备”或者在设备的具体管理界面右侧的“动作”栏中单击“Telnet”即可 Telnet 到网络设备上对其进行配置管理。

本节只是对 iMC 最基本的拓扑操作、性能管理、告警管理以及配置管理进行了简单的介绍,实际上 iMC 的功能非常强大,感兴趣的读者可以查阅《H3C 智能管理中心用户手册》以及 H3C 的官方网站 www.h3c.com.cn 上的 iMC 视频资料。

7.4.2　Cisco 设备的配置

在对 Cisco 设备的网络管理配置中，不再采用能够提供五大网络管理功能的大型网管平台，而是使用常见的免费开源网管软件，由于这些网管软件往往只能提供某一部分管理功能，因此在此对 5 大管理功能的配置分别进行介绍。

1. 网络配置管理

网络配置管理包括对网络中网络设备、网络服务等网络中各组件配置信息的管理、修改和状态监控。

（1）收集网络配置信息

网络设备配置信息保存方式及收集手段如表 7-1 所示。

表 7-1　收集网络配置信息

网络配置信息	收 集 方 式
配置文件	使用 ftp、tftp 工具传送配置文件
网络节点配置、状态信息	使用 telnet、ssh 远程登录网络设备查看配置、状态信息
MIB	使用网络管理软件通过 SNMP 代理收集配置信息

需要注意的是，通过网络访问网络设备配置信息时，建议为网络设备配置专门管理地址。同时，为保证网络设备管理地址所在接口的稳定性，一般在路由器上使用 Loopback 接口、在交换机上使用管理 VLAN 虚接口作为网络设备管理地址所在的接口。

在 Cisco PIX 防火墙上对使用 Telnet 远程访问防火墙进行严格限制。虽然防火墙任何接口都可以配置用来访问防火墙，但 Cisco PIX 防火墙要求来自外部接口的 Telnet 流量需要经过 IPSec 的保护。

在 Cisco PIX 防火墙上配置启用 Telnet 的操作步骤如表 7-2 所示。

表 7-2　Cisco PIX 防火墙 Telnet 访问配置步骤

序号	操　　作	相 关 命 令	必要
步骤 1	指定可以访问防火墙的主机	telnet	是
步骤 2	指定 telnet 访问使用的口令	passwd	是
步骤 3	指定 telnet 会话空闲时间	telnet timeout	可选
步骤 4	检查 Telnet 配置	show running-config	可选
步骤 5	管理 Telnet 会话	who kill	可选

① 指定可以访问防火墙的主机

在 Cisco PIX 防火墙上指定可以访问防火墙主机的操作为在全局配置模式下输入：

telnet {*ip-address* | *network-address*} *subnet-mask interface*

参数“*ip-address* | *network-address*”及“*subnet-mask*”用于定义哪些主机或网络可以

使用Telnet方式访问防火墙。

注意：Cisco PIX防火墙最多可支持16个主机或网络Telnet访问。

参数“interface”用于定义Telnet访问来自于防火墙的哪个接口。

例如，如下命令将定义网络192.168.1.0能够通过inside接口访问防火墙：

```
pixfirewall(config)# telnet 192.168.1.0 255.255.255.0 inside
```

② 指定Telnet访问使用的口令

在Cisco PIX防火墙上指定Telnet访问使用的口令的操作为，在全局配置模式下输入：

```
passwd password
```

③ 指定Telnet会话空闲时间

当会话空闲时断开连接，可以节省防火墙资源。在Cisco PIX防火墙上指定Telnet会话空闲时间的操作为，在全局配置模式下输入：

```
telnet timeout time
```

参数“*time*”单位为s，默认值为5。

④ 管理Telnet会话连接

在Cisco PIX防火墙上可以使用“who”命令检查有哪些主机登录到防火墙上，并可以使用kill杀掉已经连接到防火墙的Telnet连接。其操作如下所示：

```
pixfirewall# who
        0: 192.168.1.1
pixfirewall# kill  0
pixfirewall# who
```

使用“who”命令可以查看Telnet连接的连接ID，在杀掉Telnet连接时，需在kill命令后使用连接ID指定杀掉那个连接。

(2) 修改网络配置信息

修改网络节点的配置信息，可以通过两种方式进行。一种是通过远程访问，如Telnet、ssh；另一种是通过网络管理软件，例如HP OpenView等。

一般在大型网络中，会选择使用通用网络管理软件来对网络设备进行配置修改管理；大部分网络会选择使用网络设备配套的网络管理软件，对其进行管理，如Cisco路由器的SDM软件，Cisco PIX防火墙的PDM软件，Cisco交换机的Lan Manager；另外很多网络管理员仍然习惯使用Telnet或者ssh远程登录网络设备配置网络设备。

(3) 发现和显示网络的拓扑结构

网络拓扑管理是将网络设备间的连接关系以图形方式显示出来，帮助网络管理员更好管理网络。网络拓扑管理一般通过网络拓扑管理工具实现。专业的网络管理软件中一般都会设置网络拓扑管理功能。另外也有一些免费的网络拓扑发现工具，如可以在局域网中使用的LanTopolog，如图7-31所示。

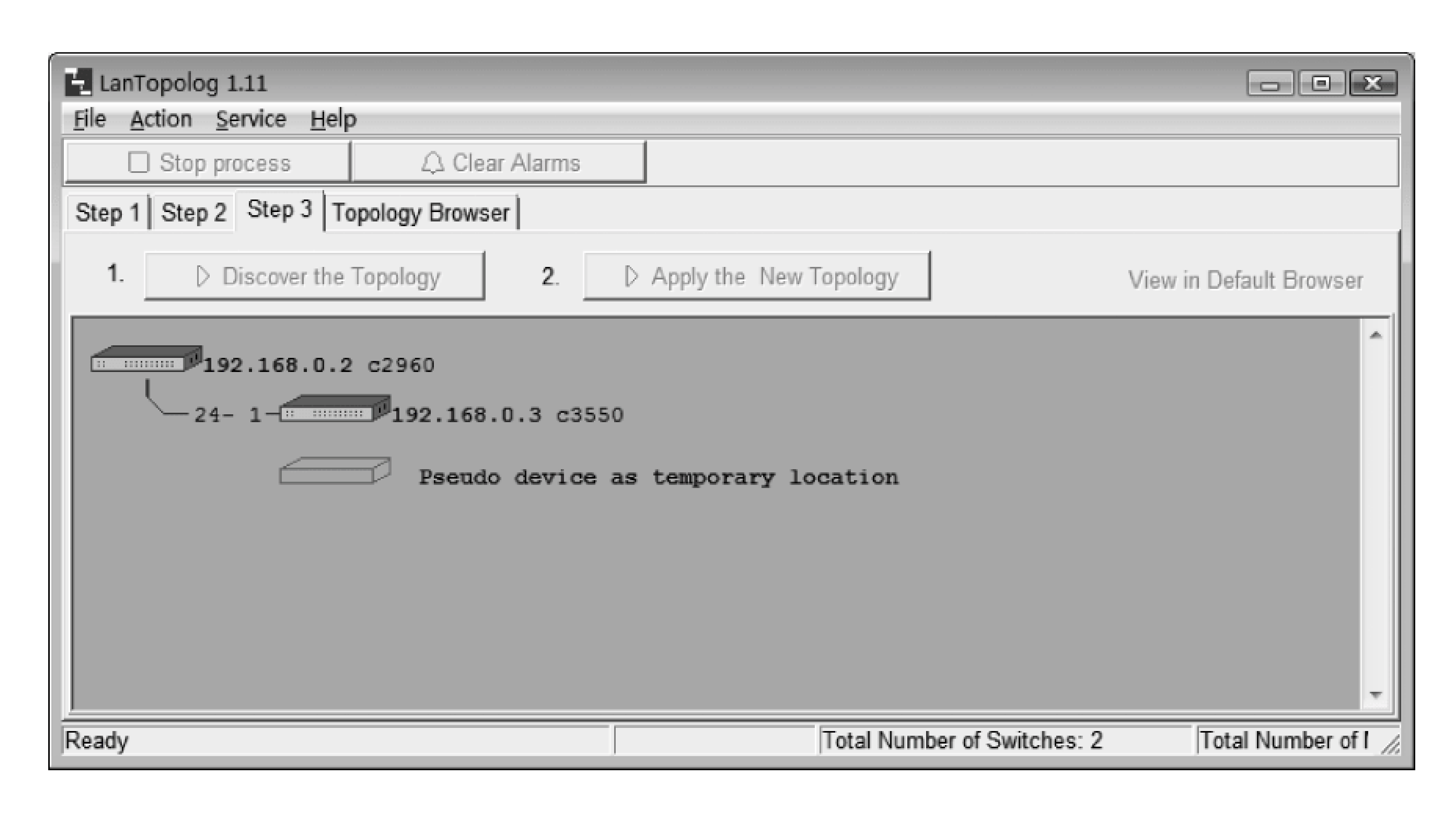


图 7-31　网络拓扑发现软件示例

2. 网络故障管理

网络故障管理的工作流程如图 7-32 所示。当发现网络出现故障时，需先收集网络故障有关数据；然后根据这些数据对网络故障原因进行分析，定位故障点、故障层次；接着应根据故障分析结果，制定故障排除方案，并对方案进行测试；如果方案经过测试可行，则可以按照方案实施排除故障；如果实施故障排除方案后还不能排除故障，则应回退重新收集故障数据，进行故障排查过程。

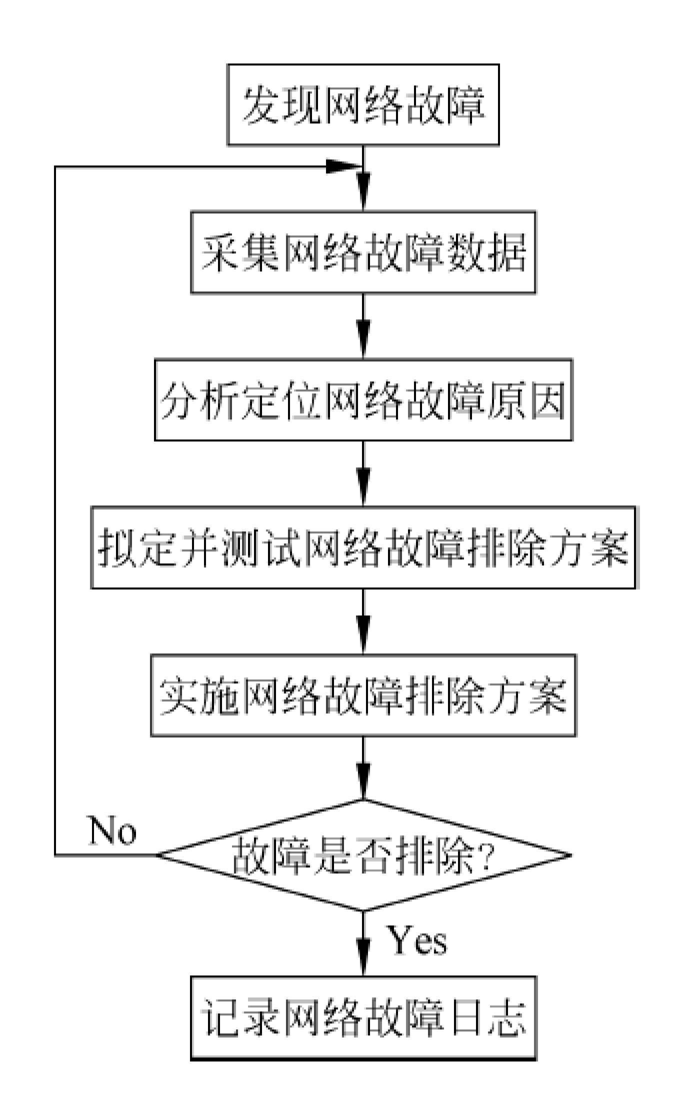


图 7-32　网络故障管理工作流程

网络管理中监测网络故障的方式有两种：异步告警、主动轮询。异步告警是指网络设备在发生故障后，主动向网络管理系统发出警报；主动轮询是指由网络管理软件定期查询网络节点状态。

网络故障分析定位的常用方法有：分层法、分段法、替换法和比较法。

（1）分层排查网络故障

计算机网络是基于 OSI 分层模型构建起来的。根据不同网络层次的功能特点，可以使用相应层次的检测工具，自上而下或自下而上逐层进行测试检查，以定位故障点。

自上而下的检查方法是指先从 OSI 模型的应用层开始检查故障原因，然后逐层向下检查；自下而上的检查方法是指从物理层开始，逐层向上排查网络故障。

一般情况下，如果根据故障现象已能够大致判断出网络层次范围时，可采用自上而下方法进行排查；当网络故障原因复杂，难以快速判断层次时，可采用自下而上的方法进行排查，由于网络上层通信需依赖下层提供的服务，所以使用该方法能够准确定位网络故障层次。

(2) 分段排查网络故障

分段排查网络故障是指以网络拓扑为参考,沿网络连接,逐段检查网络故障点的故障排除方法。分段排查时,还可使用“二分法”提高检查效率。

例如,当要排查出向网络发送大量病毒包的主机时,网络管理员常用的一种方法是逐个断掉网络上主机的网络连接,直到发现网络病毒包大量减少时,则可判定被断掉网络连接的主机被病毒入侵了。

(3) 替换法排查网络故障

替换法是指用其他的网络组件替换当前网络组件,以检测当前网络组件是否存在问题的故障排查方法。例如,排查电缆故障时,可以使用另外的线缆替换当前线缆,以检查原电缆是否出现了问题。

(4) 比较法排查网络故障

比较法是指将故障点与其他相似的网络环境进行比较,以帮助分析故障发生原因。例如,当网络中某个节点无法连接到网络时,可检查网络中其他节点情况,如果仅该节点存在网络联通性问题,则可以认为问题出在该节点上。

3. 网络安全管理

网络安全管理的工作流程如图7-33所示。进行网络安全管理的第一步是根据业务需求明确网络安全目标,制定网络安全策略;然后根据网络安全策略,对网络进行安全配置;在实施了必要的安全防护措施后,应使用网络安全审查工具定期对网络安全性进行检查和测试;如果发现网络存在安全漏洞,则需要修改、完善网络安全配置;另外,除主动进行的安全审查外,当发生的网络安全事件证明网络还存在安全漏洞时,也要对网络安全配置进行修改、完善。

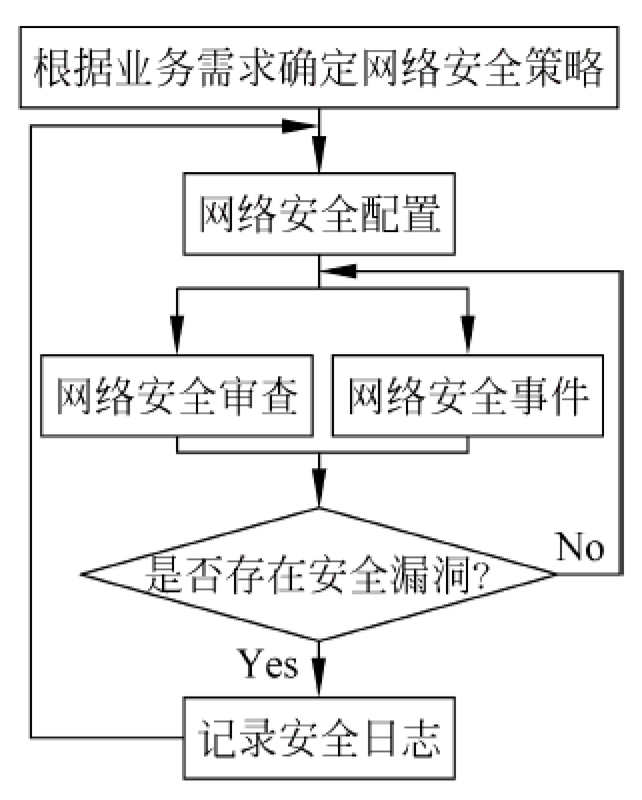


图7-33 网络安全管理工作流程

(1) 网络安全审查

网络安全审查是指根据网络安全需求和网络安全标准对网络进行网络安全风险检查、评估的过程。目前有很多专门的网络安全漏洞扫描软件,如Nessus、SAINT等,可以对各种操作系统、网络设备进行安全漏洞扫描。

Nessus软件可以扫描网络上的主机、网络设备,并将其与所存的安全漏洞定义库进行比较,检查其是否在访问控制、系统bug等方面存在安全漏洞。图7-34所示为使用Nessus对某系统进行扫描后的结果。

Nessus检查结果中会给出安全漏洞对应的风险标识号,检索CVE、BID、OSVDB等安全漏洞网站,可以查看到该风险标识号对应的解决建议。CVE、BID、OSVDB等就像字典表,会为广泛认同的信息安全漏洞、已经暴露出来的弱点、已经发现的蠕虫等给出一个公共的名称。

(2) 入侵检测和入侵防御

入侵检测是一种用于发现网络入侵行为的技术,提供入侵检测功能的系统称为入侵检测系统(IDS)。入侵检测系统通过检查所收集网络数据报文是否具有入侵特征或网络是否出现异常,来判断是否网络是否受到入侵。入侵检测系统一般以旁路方式接入在高

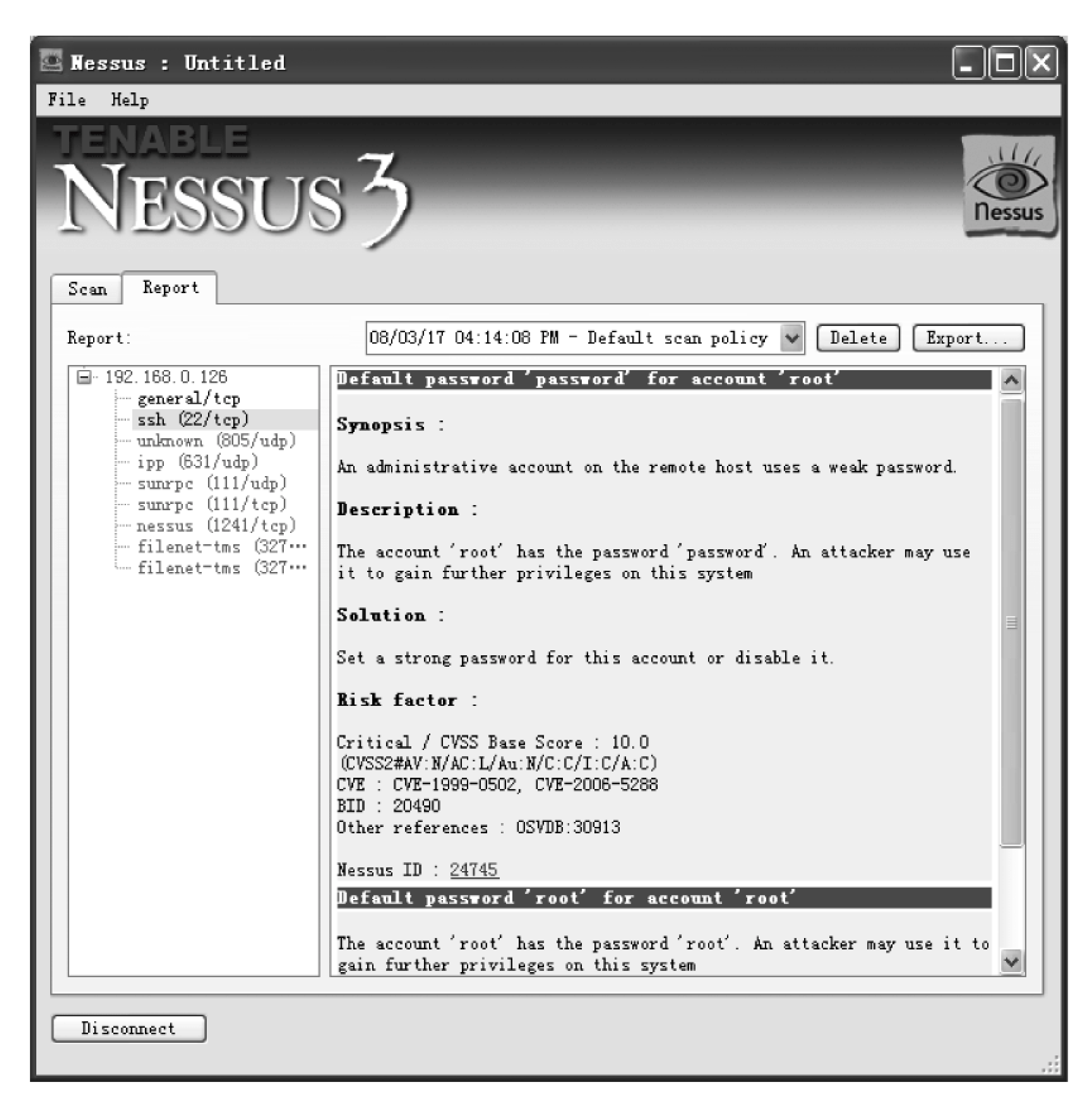


图 7-34　Nessus 安全扫描结果

安全等级网络入口处，如图 7-35 所示。

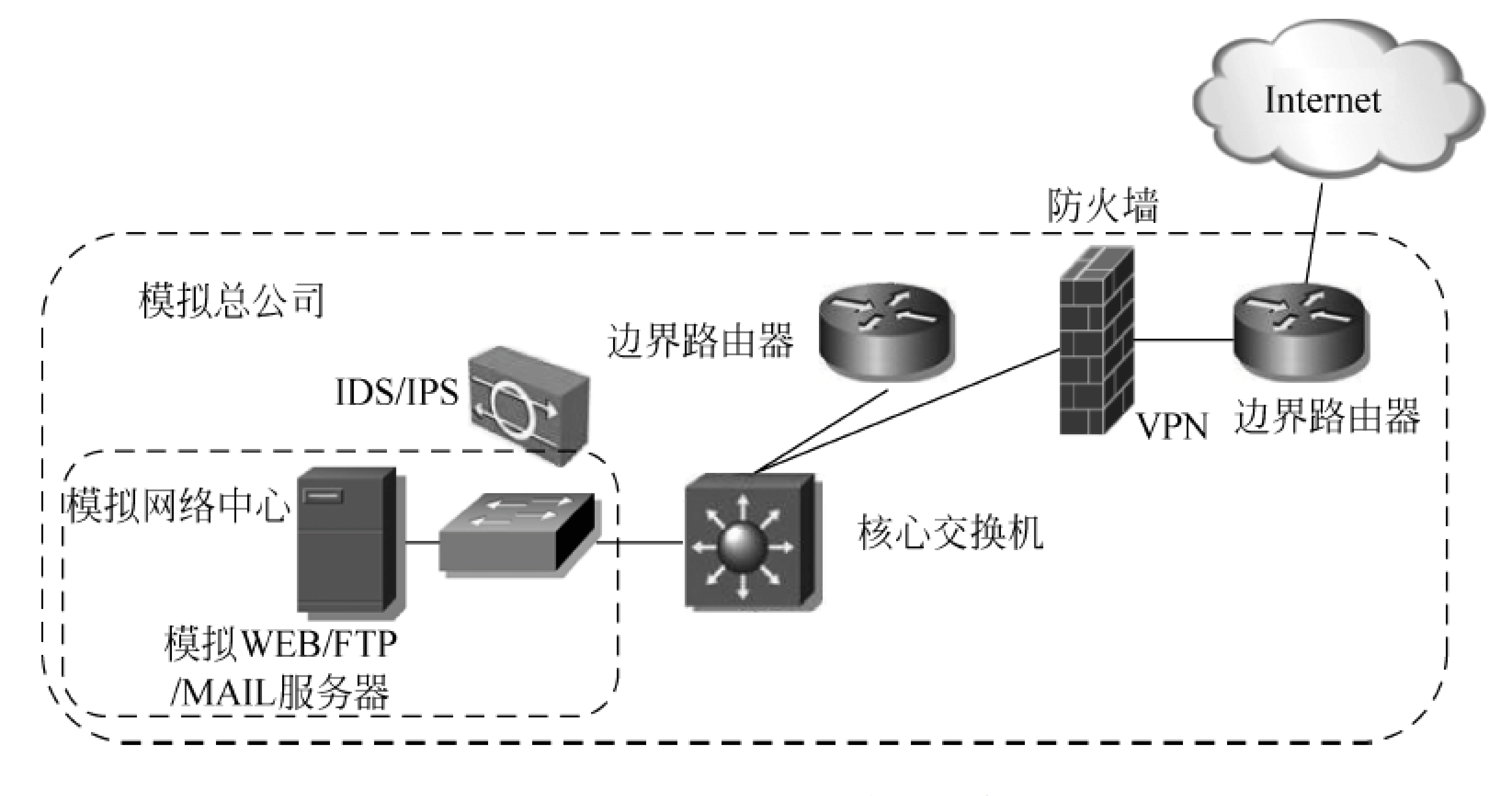


图 7-35　IDS/IPS 接入示例

入侵防御(IPS)技术是能够发现网络入侵行为并进行自防御的技术。相对 IDS，入侵防御在发现入侵后，会发出警报、丢弃数据包和重置连接。

(3) 防病毒技术

随着网络的普及和计算机病毒的发展,目前的计算机病毒侵害的对象不再只是单台主机,而是整个网络。所以网络安全管理,尤其是局域网安全管理中一项重要的工作是进行病毒防护布控。

目前常见的网络病毒种类如下。

① 系统病毒:感染特定的操作系统中的文件,例如 Windows 系统中的 *.exe 和 *.dll 文件,并通过这些文件进行传播。例如,CIH 病毒。防病毒软件通常使用 Win32、PE、Win95 等作为前缀定义该类病毒。

② 蠕虫病毒:通过网络或者系统漏洞在网络上进行传播,阻塞网络。例如,冲击波病毒、小邮差病毒。防病毒软件通常使用 Worm 作为前缀定义该类病毒。

③ 木马病毒:该类病毒的特点是通过网络或者系统漏洞进入用户系统并将自己隐藏起来,然后向外界泄露用户信息。防病毒软件通常使用 Trojan 作为前缀定义该类病毒。

④ 黑客病毒:该类病毒也是通过网络或者系统漏洞进入用户系统并将自己隐藏起来,但黑客病毒不仅泄露用户信息,还使用户主机可被黑客远程控制。防病毒软件通常使用 Hack 作为前缀定义该类病毒。

⑤ 脚本病毒:通过网页传播,以 VBS、JavaScript 等脚本语言编写。防病毒软件通常使用 Script 作为前缀定义该类病毒。

⑥ 宏病毒:是一类特殊的脚本病毒。通过微软 Office 处理的文件进行传播。防病毒软件通常使用 Macro 作为前缀定义该类病毒。

⑦ 后门病毒:与木马病毒相似,通过网络传播,一旦侵入用户系统,则在系统上打开系统后门(某些监听端口)。防病毒软件通常使用 Backdoor 作为前缀定义该类病毒。

目前主要的防病毒技术如下:

① 基因码检测技术:基因码检测也被称为特征码检测。目前几乎所有防病毒软件主要使用的还是此种技术。其原理是利用病毒数据库里的病毒特征数据,与被扫描文件进行对比,从而找出被病毒感染的文件。但使用这类防病毒技术能够有效查杀病毒的基础使病毒库能够及时得到更新,病毒库中能收录最新的病毒特征数据。

② 虚拟机技术:虚拟机技术是指防病毒软件在进行查杀病毒时,模拟出一个小型虚拟运行环境,让程序在该虚拟运行环境中试执行,从而使病毒暴露其攻击特征。使用此种技术可以发现大部分变形病毒和大量未知病毒。

③ 代码分析技术:通过分析指令出现顺序或特定代码组合等病毒特征来判断文件是否感染病毒的技术。即通过扫描病毒特定的行为或多种行为组合来判断文件是否感染了病毒。

④ 主动防御技术:主动防御技术是指全程监视进程行为,发现“违规”行为,就通知用户或直接终止进程的技术。通过监控 Windows 系统的注册表键值、系统文件、网络访问等变动情况,发现是否受到病毒侵害。其缺点是需要用户太多干预。

(4) 记录安全日志

通过安全日志,网络管理员可以获得网络安全事件的许多信息,但记录安全日志会消

耗网络设备的网络资源，因此需在网络性能许可下谨慎配置。要记录网络节点的日志，需先安装配置 Syslog 服务器，然后在网络节点上启用日志记录功能。

① 配置网络设备记录日志。在 Cisco 网络设备上配置进行日志记录的基本步骤如表 7-3 所示，日志级别参数值如表 7-4 所示。

表 7-3　启用网络设备安全日志功能的基本步骤

序号	操　　作	相 关 命 令	必要性
步骤 1	启用日志记录功能	logging enable 或 logging on	是
步骤 2	指定 syslog 服务地址或主机名	logging host	是
步骤 3	指定日志级别	logging trap	是

表 7-4　日志级别参数值

级别值	日志级别	含　　义
0	emergencies	系统不可用
1	alerts	报警，在端口上需要立即操作
2	critical	网络设备上存在一个关键状态
3	errors	网络设备上存在一个错误状态
4	warnings	网络设备上存在一个警告状态
5	notifications	网络设备上发生了一个重要的事件
6	informational	网络设备上发生了一个信息事件
7	debugging	来自 debug 命令的输出

例如，要将边界路由器日志写入到 200.100.8.25 上的配置操作如下：

```
zb-r0(config)#logging on
zb-r0(config)#logging host 200.100.8.25
zb-r0(config)#logging trap informational
```

② 安装配置日志服务器。Kiwi Syslog Daemon 是一种常用的 Syslog 服务器。Kiwi Syslog Daemon 安装完成后，还需配置服务监听的地址和端口。运行 Kiwi Syslog Daemon，单击软件快捷菜单上的 ☑ 图标，打开如图 7-36 所示配置窗口，配置服务监听的地址和端口。

在“Bind to address”处输入 Syslog 服务器使用的地址。

当服务器在正确的地址和端口上开始监听日志记录请求时，网络设备上会出现如下提示信息，表示目前设备正在连接 Syslog 服务器，一旦连接成功，会在 Syslog 服务器主窗口中能看到网络设备发来 log 信息。

```
*Sep  5 19:13:02.423: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 200.100.
8.25
started - CLI initiated
*Sep  5 19:13:02.423: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 200.100.
8.25
started - CLI initiated
```

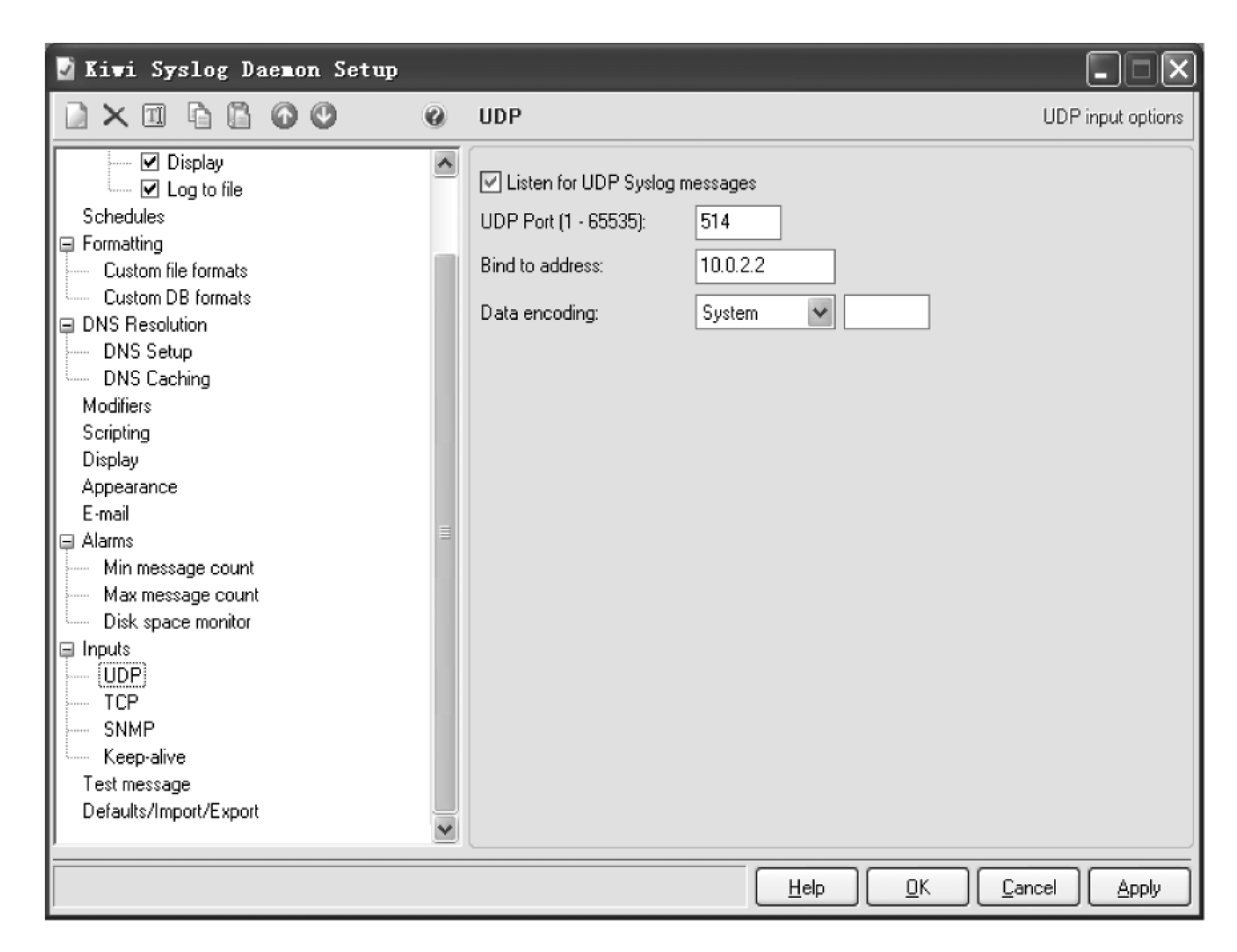


图 7-36 配置 Syslog 服务器监听地址和端口

4. 网络性能管理

计算机网络由网络设备、线路、网络服务等构成,网络性能管理需要对这些网络组件的运行状态、效率进行监控和调整,使网络能在满足通信需求的情况下更高效的工作。网络性能管理的工作流程如图 7-37 所示,其中采集、分析网络性能数据也被称为网络性能监控。

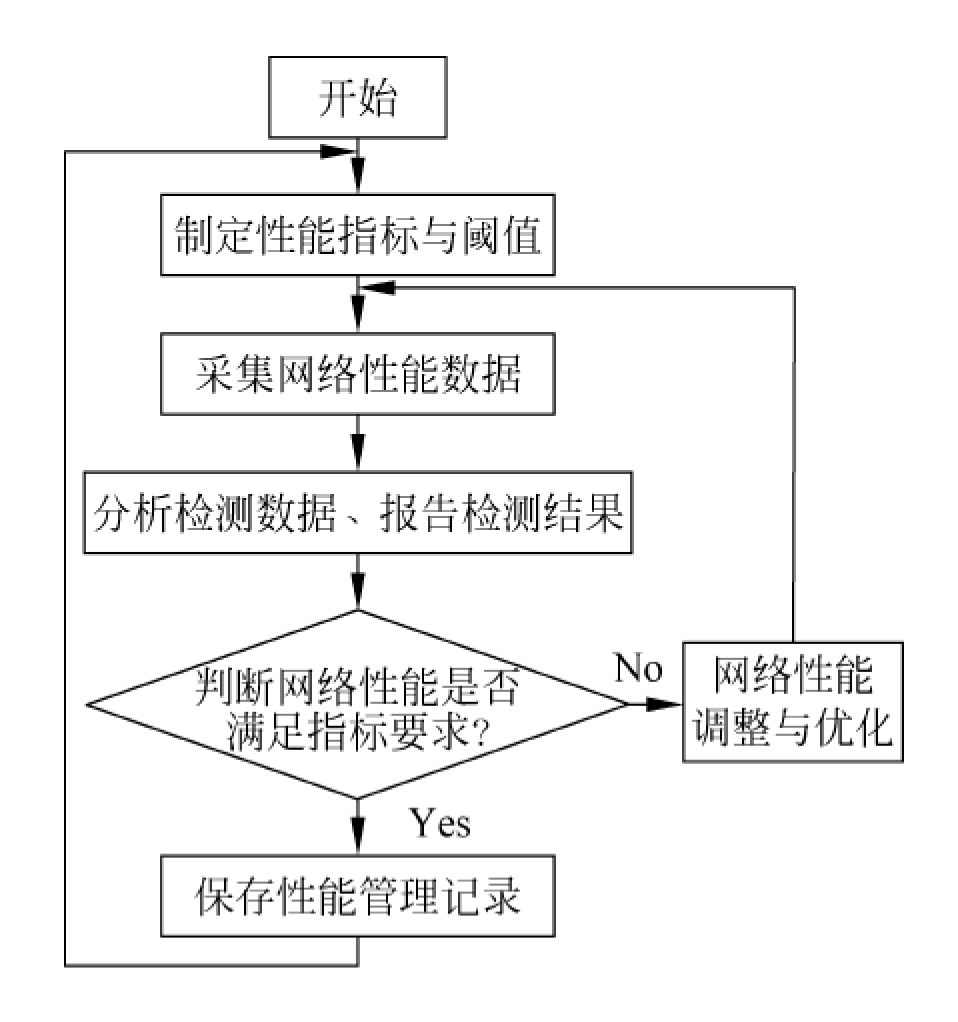


图 7-37 网络性能管理工作流程

（1）网络性能指标

评价网络性能通过评价网络是否满足某些性能指标来进行。常用网络性能指标包括以下几种。

① 网络总体性能指标：网络联通性、网络吞吐量、网络资源利用率、响应时间等。

② 网络节点性能指标：吞吐量、转发率、丢包率、节点处理时延等。

③ 链路性能指标：带宽、信道利用率、带宽利用率等。

④ 网络服务的性能指标：服务响应时间、最大并发连接数等。

（2）采集网络性能数据的方法

采集网络性能数据可从以下 3 个方面进行。

① 利用驻留在网络节点上的网络管理代理程序，采集网络性能数据。例如，通过配置网络设备上的 SNMP 代理，可以读取网络设备上 MIB 中有关网络性能的信息。

② 观察网络现有流量。例如，可通过网络监听工具（Wireshark、Sniffer 等）捕获网络上现有数据包，分析数据报文是否存在广播风暴、是否有大量重传的数据包等，从侧面了解网络当前性能状况。

③ 制造测试流量，并观察网络处理测试流量的情况。例如，可通过观察到某网络节点的 ping 包响应返回时间延迟，来获得两个网络节点间的网络时延信息。

（3）利用网管代理检测网络性能

目前常用的网络设备或主机操作系统都支持 SNMP 网络管理功能。通过配置网络设备和主机上的 SNMP 代理程序，使网管工具能够利用 SNMP 协议从网络设备或主机上直接采集网络性能数据，监控网络性能。

在 Cisco IOS 路由器或交换机上配置 SNMP 代理涉及的命令如下：

① 定义 SNMP 共同体。

```
Router(config)#snmp-server community community-name {ro|rw}
```

② 指定网管工作站的地址，即 Trap 的目标主机地址。

```
Router(config)#snmp-server host ip-address community-name
```

例如，如果基于 SNMP 的网络监控软件安装在主机 192.168.0.254 上，而 snmp 共同体名为 test，则可以在网络设备上输入如下命令创建相应 SNMP 共同体，并定义网络设备网络管理代理所对应的管理实体地址：

```
C2960-1-2-1(config)#snmp-server community test
C2960-1-2-1(config)#snmp-server host 192.168.0.254 test
```

③ 启动 SNMP 的 Trap 功能。

```
Router(config)#snmp-server enable traps
```

在配置完成后，可以使用 show snmp 命令检查网络设备上 SNMP 代理的配置信息。具体命令执行结果如下：

```
C2960-1-2-1#show snmp community
```

```
Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only active

Community name: test
Community Index: cisco1
Community SecurityName: test
storage-type: nonvolatile active
```

执行 show snmp host 命令查看网络设备上配置的网络管理实体地址信息,显示结果如下:

```
C2960-1-2-1#show snmp host
Notification host: 192.168.0.254        udp-port: 162    type: trap
user: test        security model: v1
```

在配置完 SNMP 代理后,还需要安装和配置相关的网管软件进行网络性能管理。在此对 PRTG 软件的安装和配置进行介绍。PRTG 是一款基于 Windows 平台的网络性能监控软件。它能够通过 SNMP 协议与网络节点上的网络管理代理通信,获取网络节点上的 MIB 信息,并通过图表方式显示出来。

从"www.paessler.com/prtg/download"可以下载 PRTG 的免费试用版。其安装非常简单,只需双击运行安装程序,然后配置几项参数,逐步单击 Next 按钮即可。PRTG 安装过程中需要配置的参数,如图 7-38 所示。

图 7-38　PRTG 监控服务器配置窗口

① PRTG 监测服务器工作的 IP 地址。由于最新支持 Web 页面显示功能的 PRTG，需要在 Windows 系统上创建一个 Web 服务器来显示 PRTG 获取的网络性能数据，所以在安装过程中，需输入该服务器工作的 IP 地址。

② 网络管理员邮件地址。PRTG 支持多种向网络管理员报告网络性能信息的方式，如电子邮件等，所以在安装过程中，还需输入网络管理员的电子邮件地址。

③ 登录 PRTG 的账号。PRTG 内嵌一个登录账号为“prtgadmin”，口令为“prtgadmin”。也可以在安装过程中设置使用其他账号来登录 PRTG。

安装完成后，需要对 PRTG 进行配置。首先双击 Windows 桌面上的 PRTG 图标，然后在图 7-39 所示的窗口中输入管理账号“prtgadmin”和口令登录 PRTG。

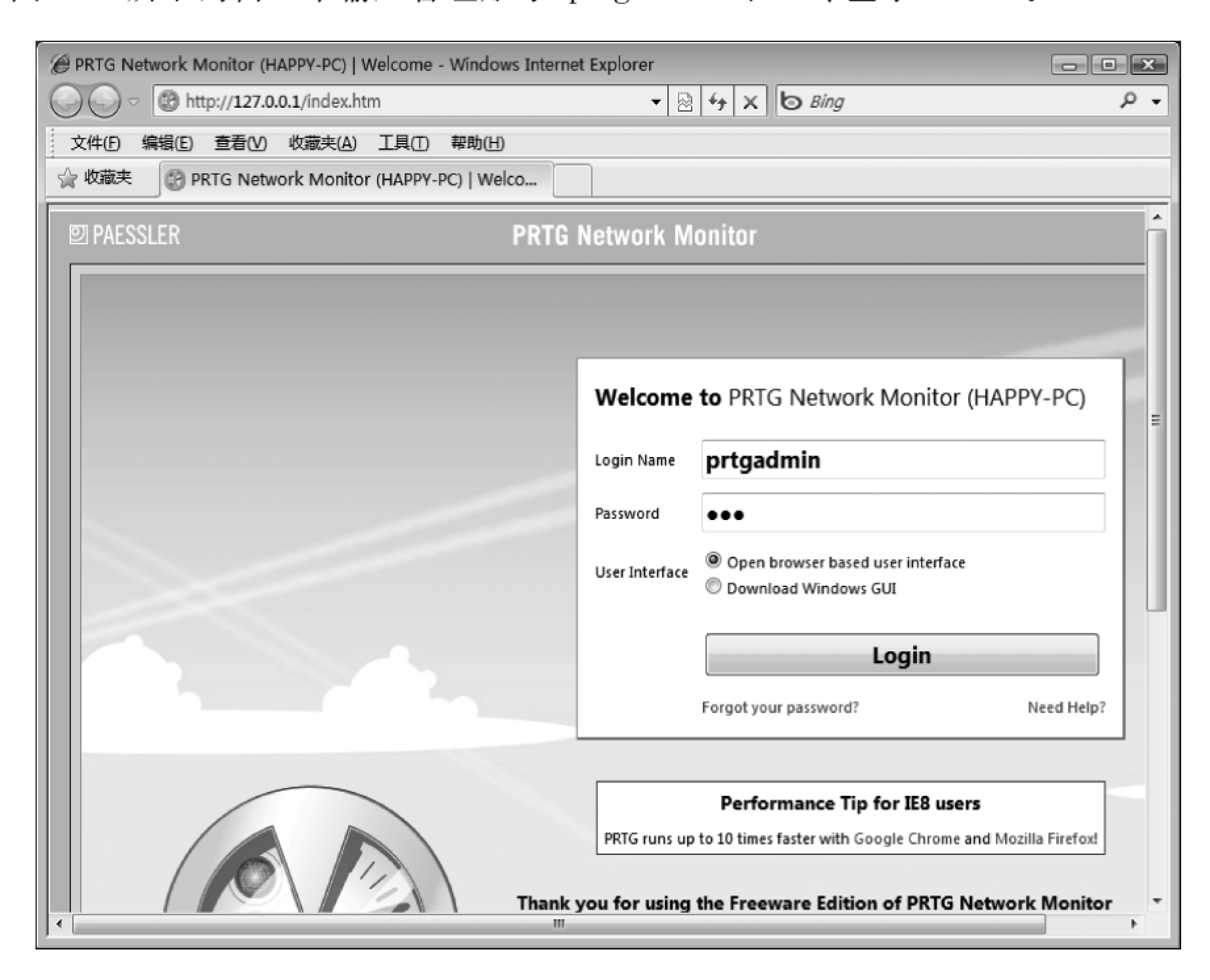


图 7-39 登录 PRTG 窗口

登录 PRTG 后的主窗口如图 7-40 所示。单击窗口中的 Add Sensor(s) Manually 图标，为所要管理的设备创建新的感应器 Sensor。

在接下来的图 7-41 所示的 PRTG 窗口中，先单击 Create a new Device 单选按钮，然后单击 Continue 按钮，选择为被管设备创建一个设备条目。

由于 PRTG 使用将被管对象进行分组管理，所以还需在图 7-42 所示窗口中，单击 Create a new Group 单选按钮，然后单击 Continue 按钮，选择新建一个组。

PRTG 接下来显示图 7-43 所示窗口，为组配置默认属性。例如与管理代理程序通信使用的 SNMP 共同体名、SNMP 协议版本、通信端口等。

完成组的创建操作后，PRTG 会显示图 7-44 所示组列表窗口，在其中选择新创建的组，单击该组下面的 Add Device 按钮，将进入图 7-45 所示创建新设备条目窗口。



图 7-40　PRTG 主窗口

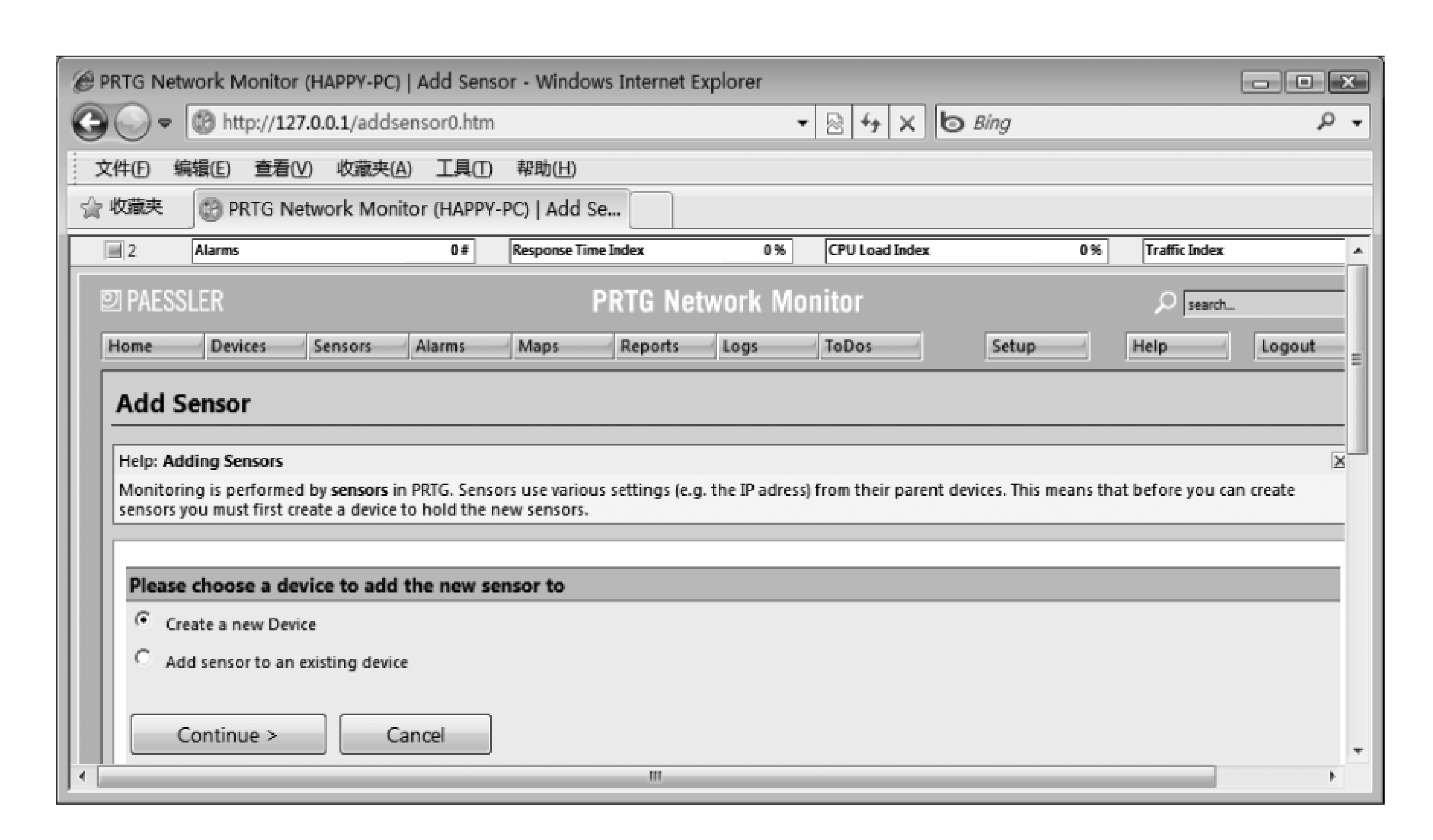


图 7-41　新建设备窗口

在图 7-45 所示窗口中，必须配置的是 SNMP 通信属性。取消选中 Inherit Credentials of SNMP Devices 复选框，并在展开的窗口中，输入与管理代理程序通信使用的正确的 SNMP 共同体名，然后单击 Continue 按钮即可创建新设备条目。

完成设备条目创建后，需要创建探测器 Sensor，才能监测网络设备上接口、链路的性能配置。在图 7-46 所示组列表窗口中，选择设备条目，单击其右侧的 Add Sensor 按钮可

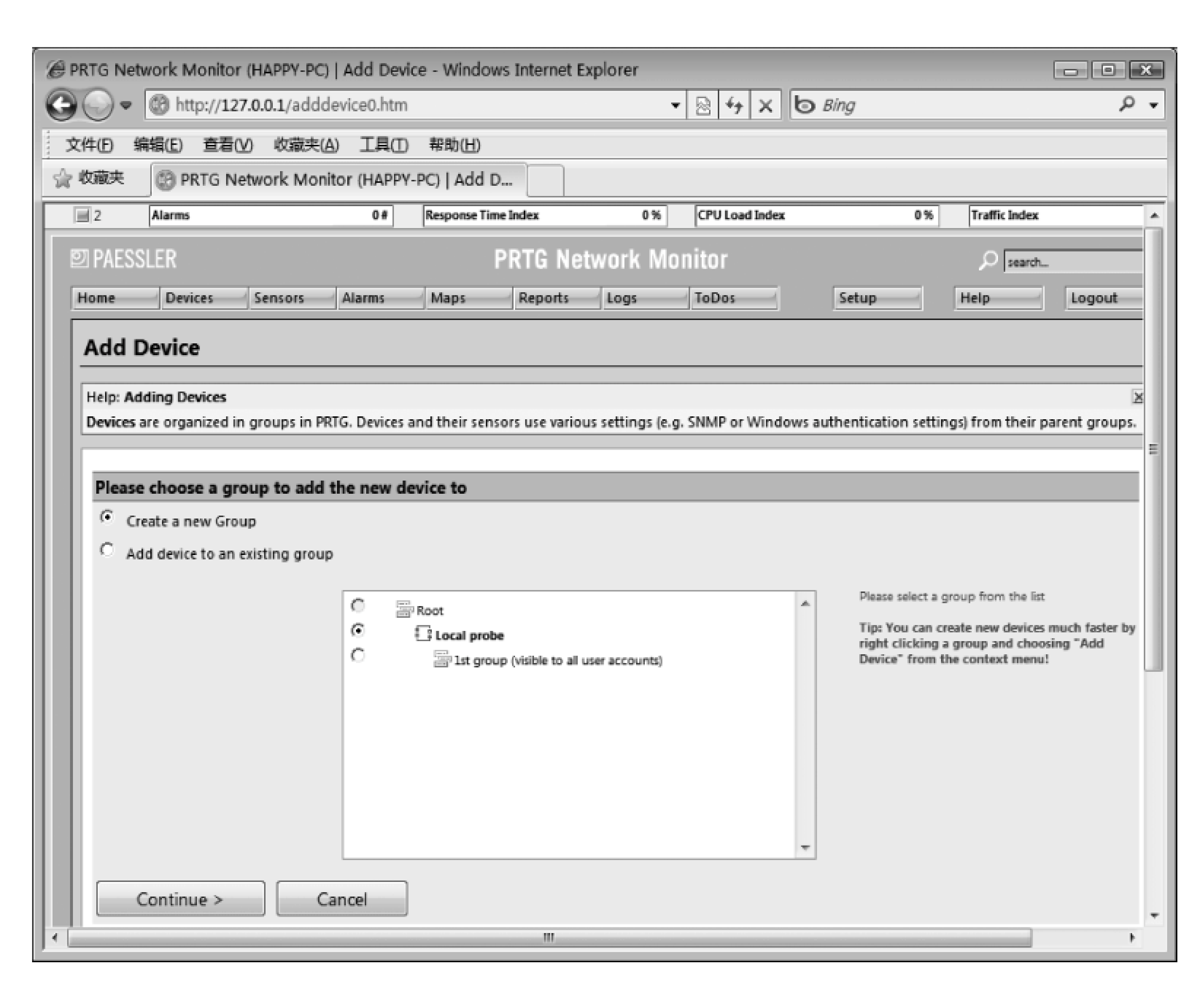


图 7-42　新建组窗口

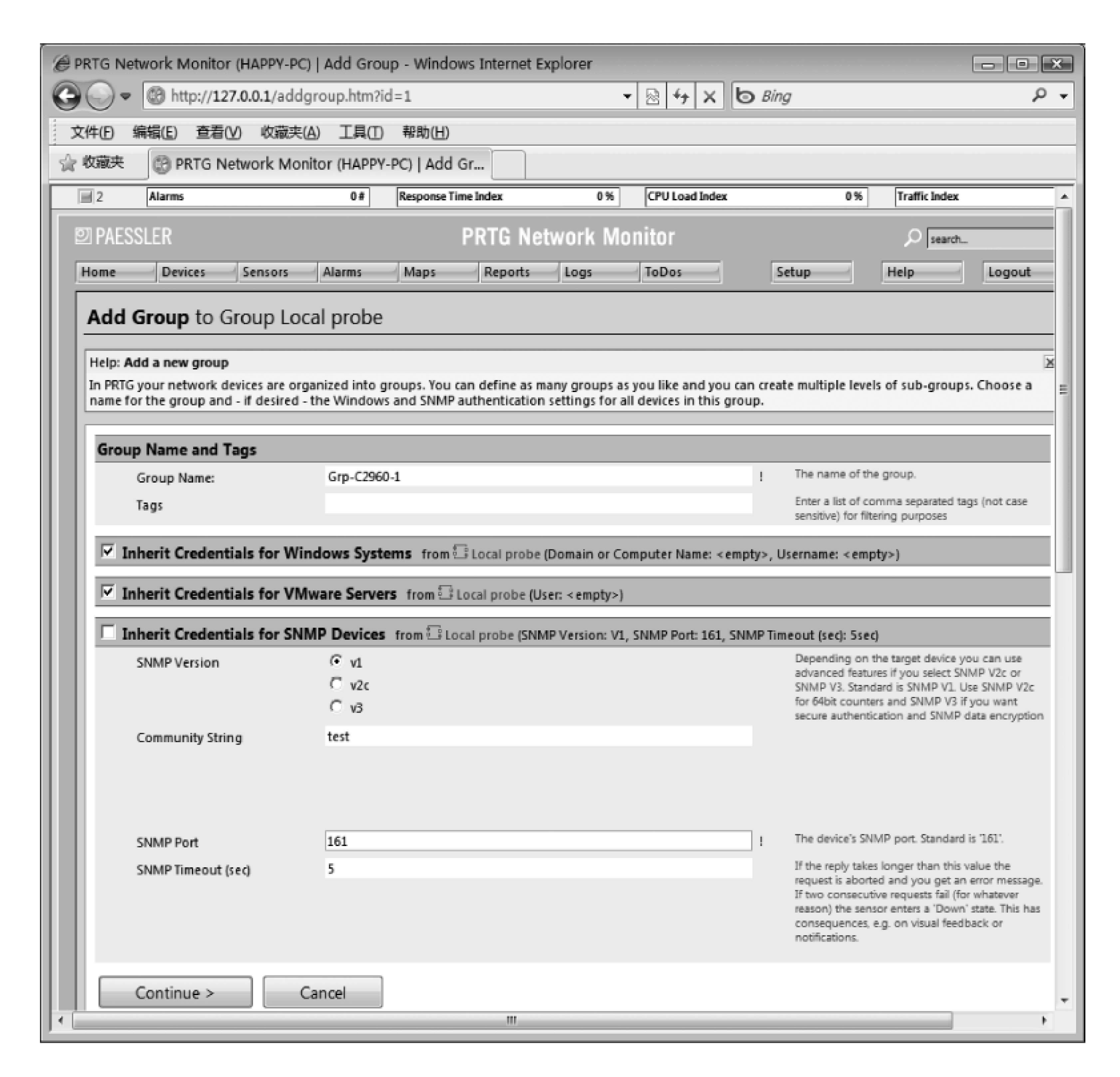


图 7-43　配置组的 SNMP 属性

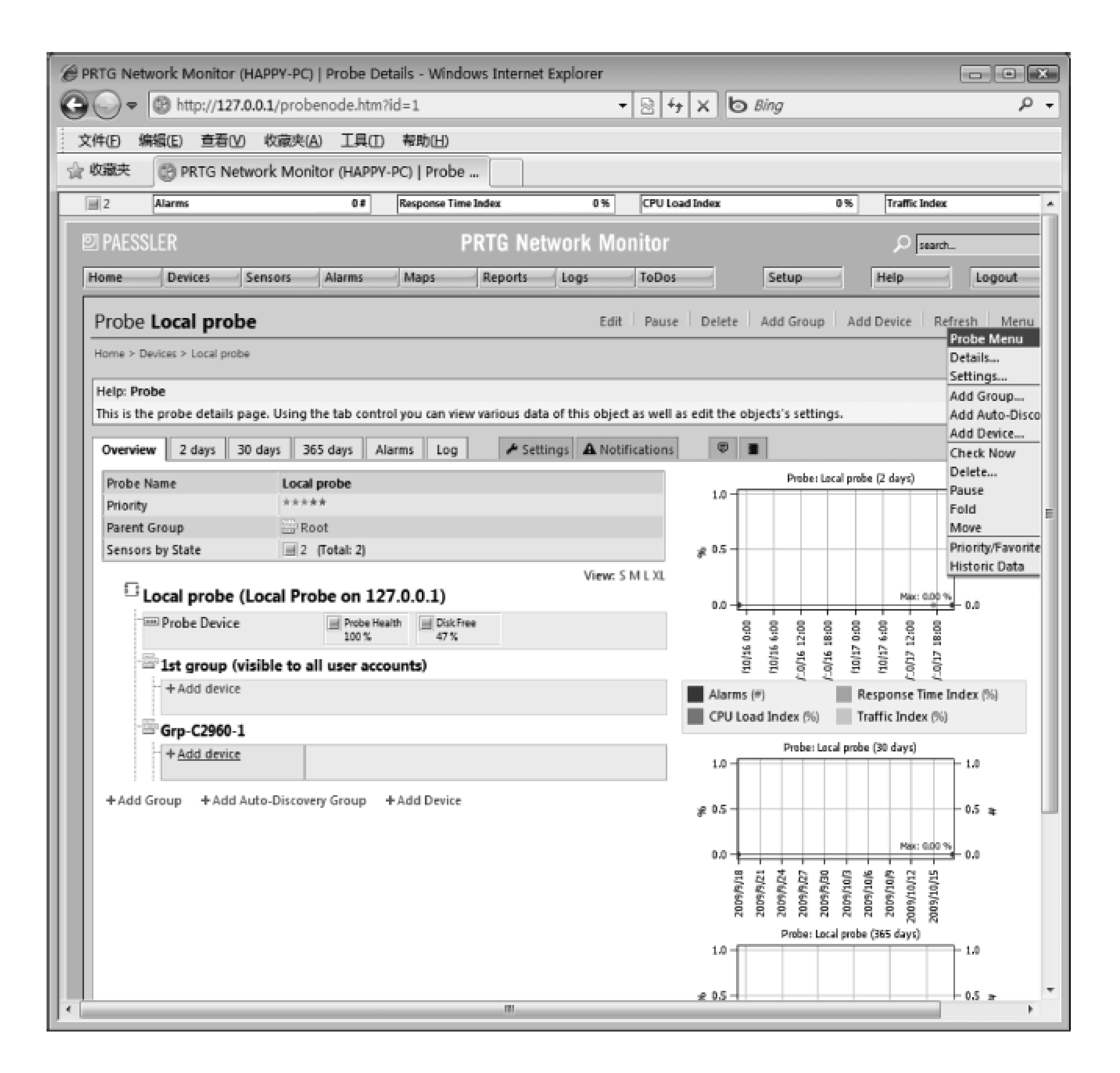


图 7-44 在组中添加设备

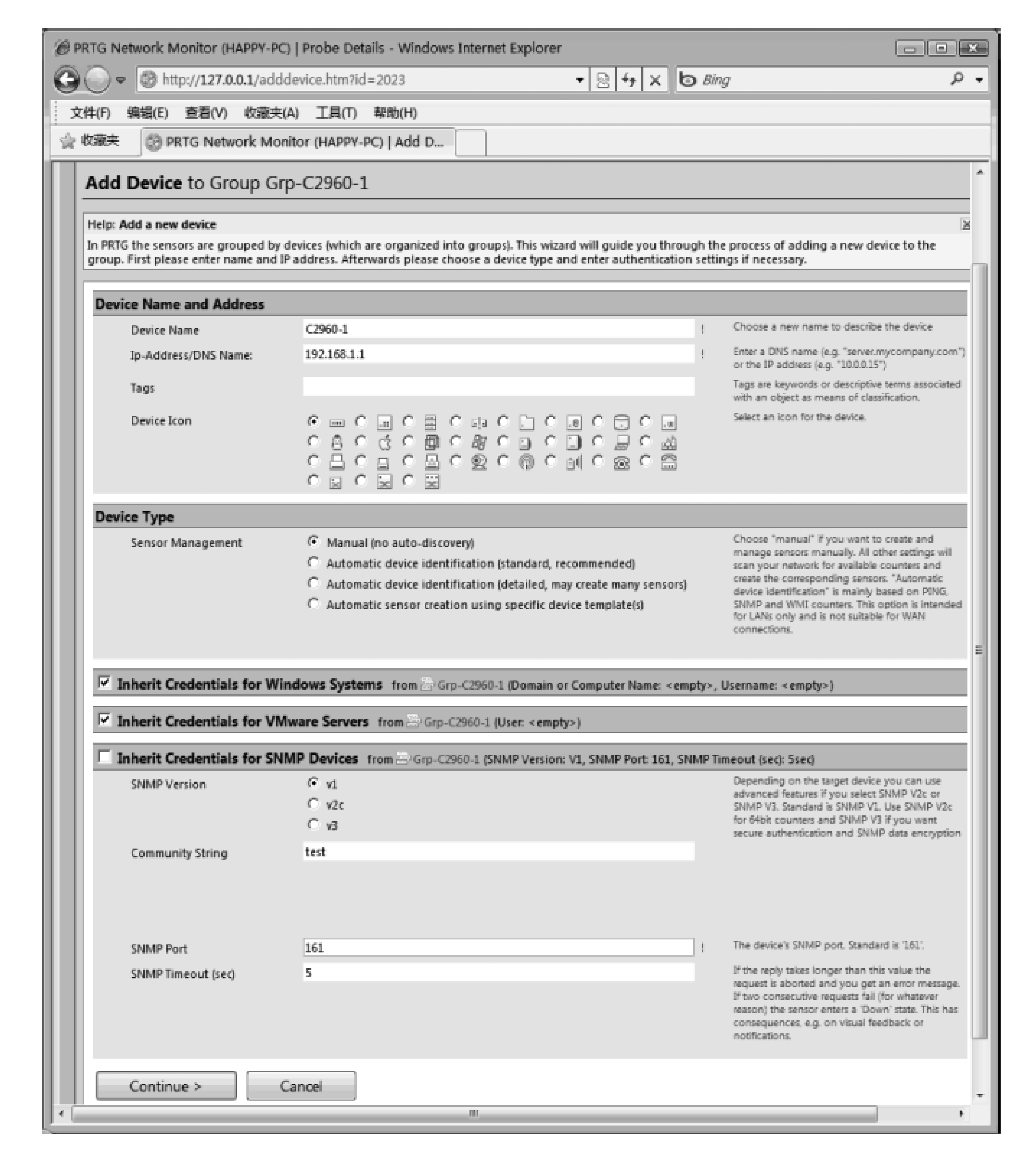


图 7-45 创建新设备相关属性

以为其创建 Sensor。

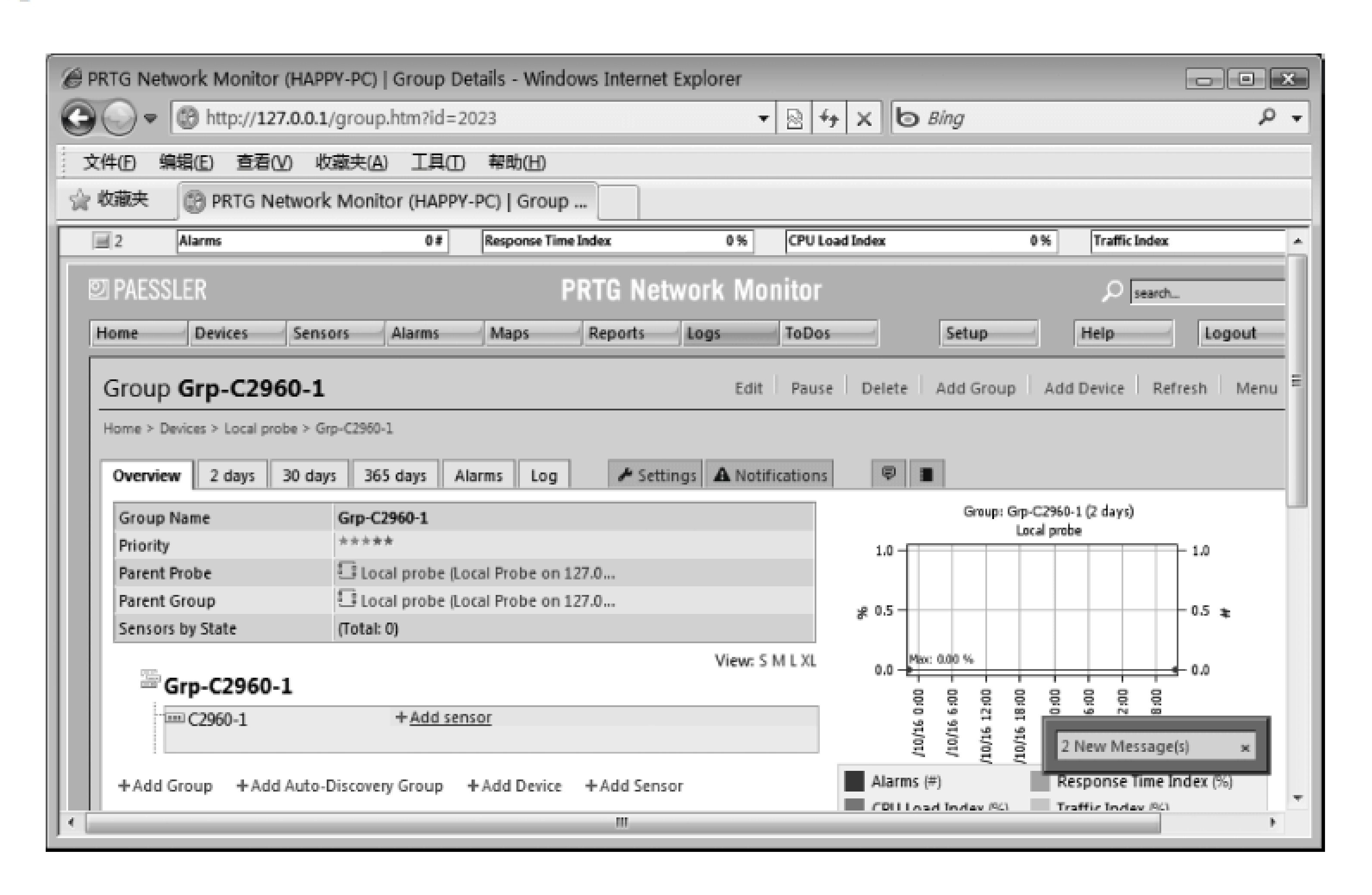


图 7-46　为新设备添加探测器

在创建 Sensor 窗口中，单击展开 SNMP 菜单，选择创建使用 SNMP 协议获取信息的探测器。注意，由于 Cisco 网络设备需要使用其自己扩展的 MIB，所以要在 SNMP 探测器菜单中单击 SNMP Library 选择探测器使用的 MIB，如图 7-47 所示。PRTG 附带了两个 Cisco MIB，一个是 Cisco Interface MIB，另一个是 Cisco Queue MIB。选择 Cisco 设备默认支持的 Cisco Interface MIB，单击 Continue to step2 按钮，连接网络设备。

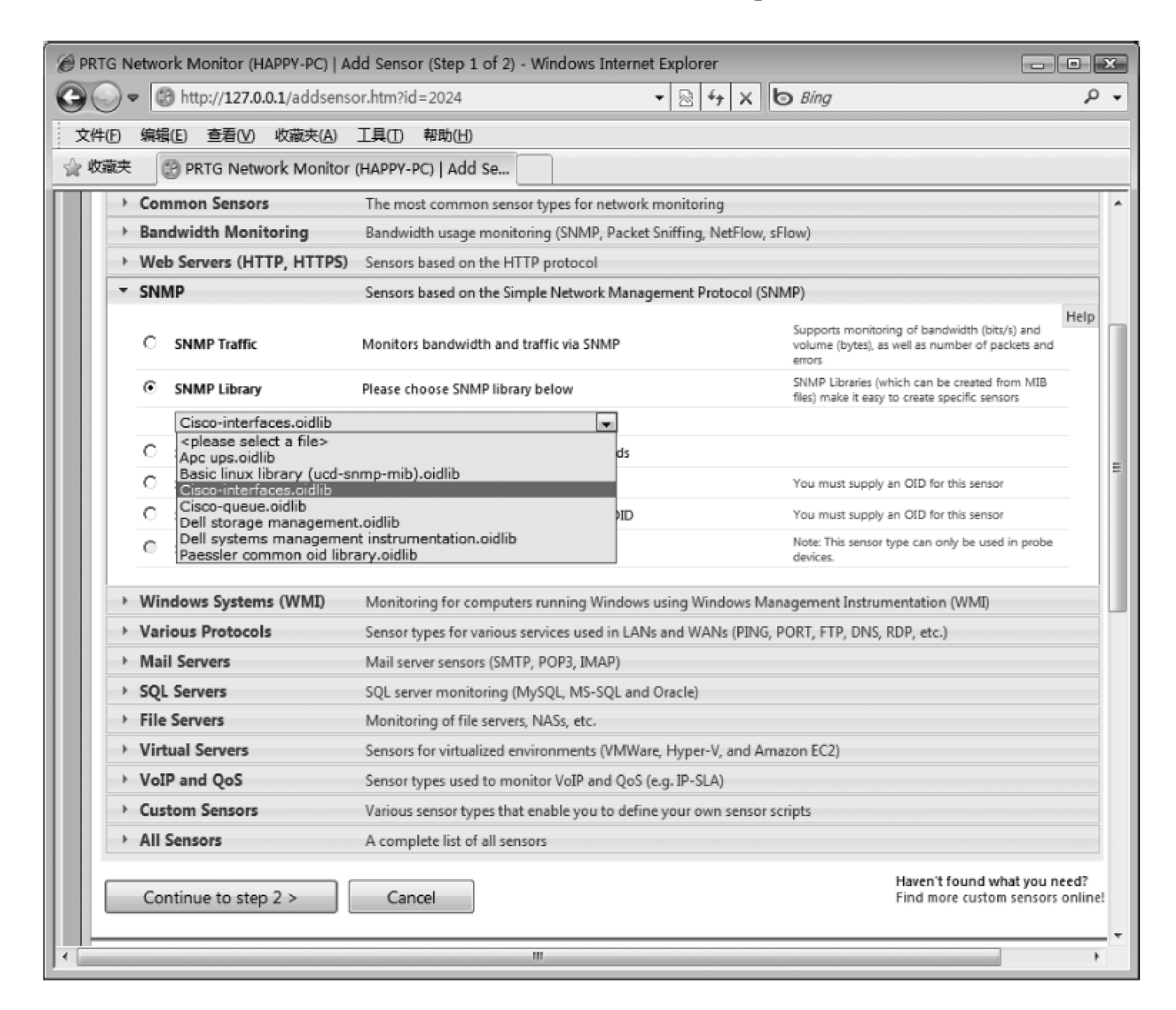


图 7-47　定义探测方式

在PRTG使用正确的SNMP共同体名连接到网络设备后,会显示图7-48所示窗口,供管理员选择要探测的配置信息。该窗口中显示在网络设备MIB中的被管理对象信息条目,如if Index,即网络设备接口的索引号。在图7-48所示窗口中选择想要探测的网络设备信息条目,单击窗口下方的"Continue"按钮,则PRTG会根据所选生成相应的探测数据,显示在图7-49所示窗口中。其中一条被监测设备的信息条目被称为一个Sensor。

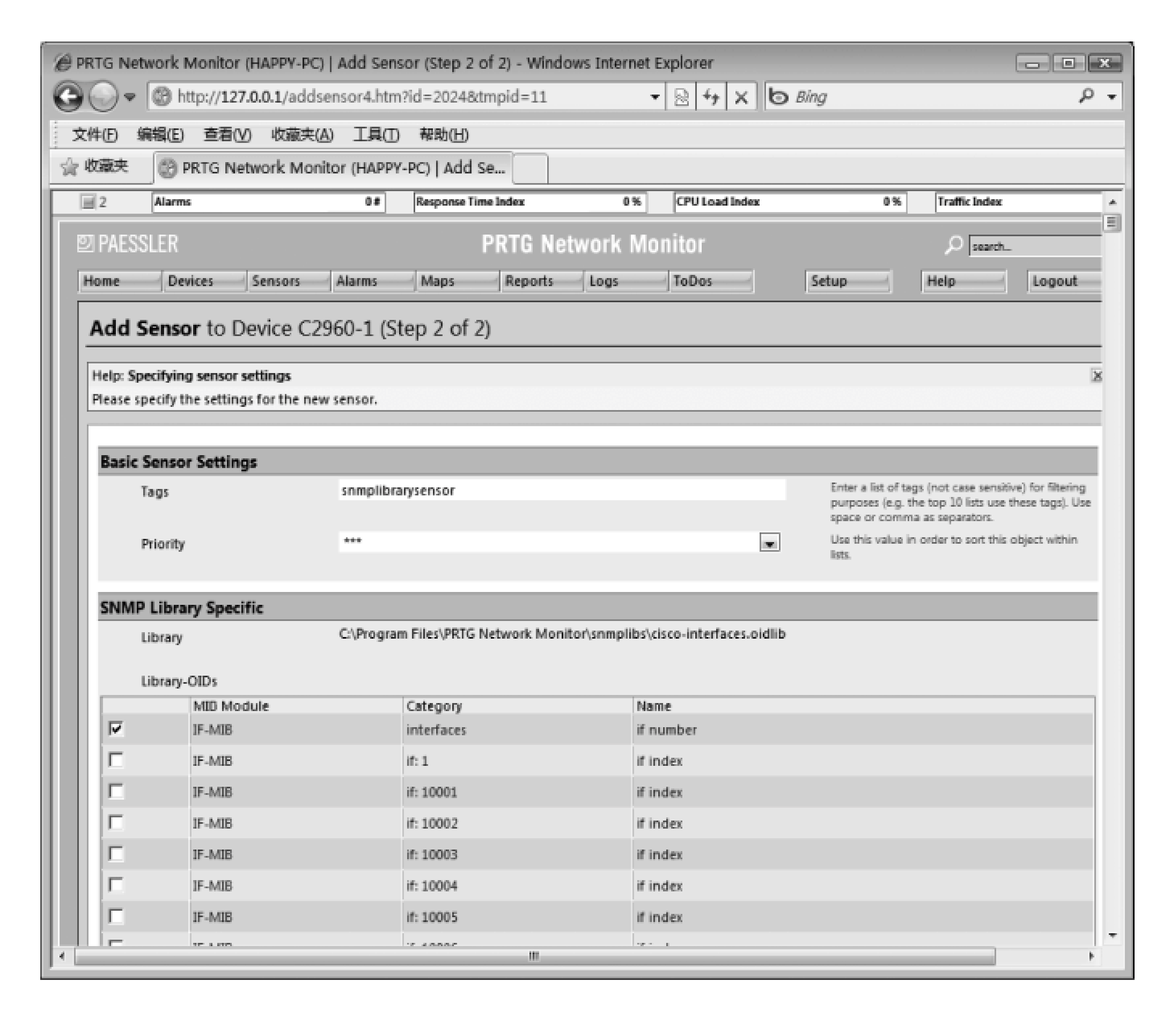


图7-48 选择要探测的配置信息

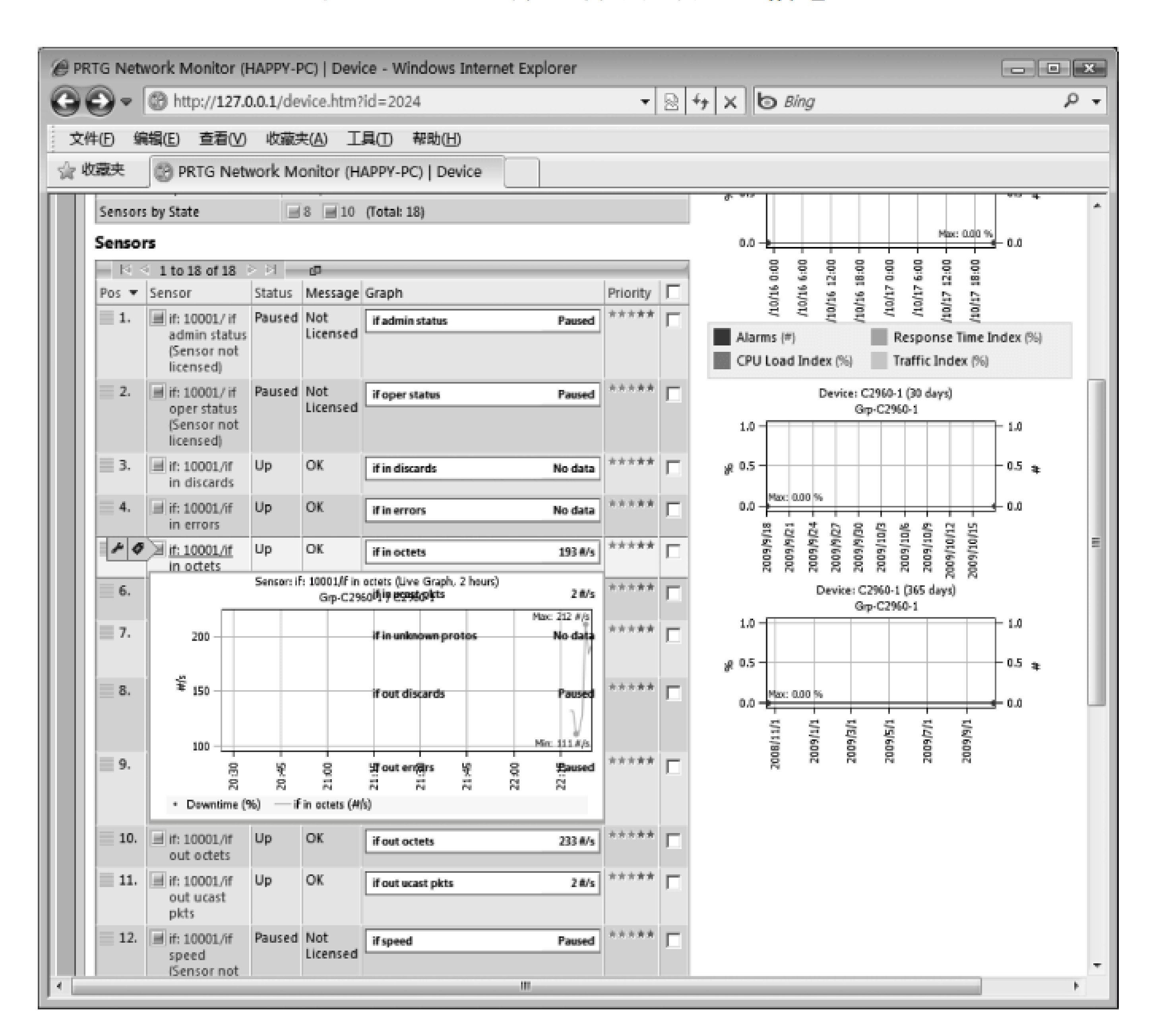


图7-49 PRTG监测到的网络设备信息

在图 7-49 所示窗口中，单击被监测的探测器，则会打开图 7-50 所示窗口，显示该探测器监测到的探测数据。通过这些探测数据，可以了解网络接口上的数据流量变化，并根据其应有的指标阈值，确定网络是否出现了拥塞、断路等情况。

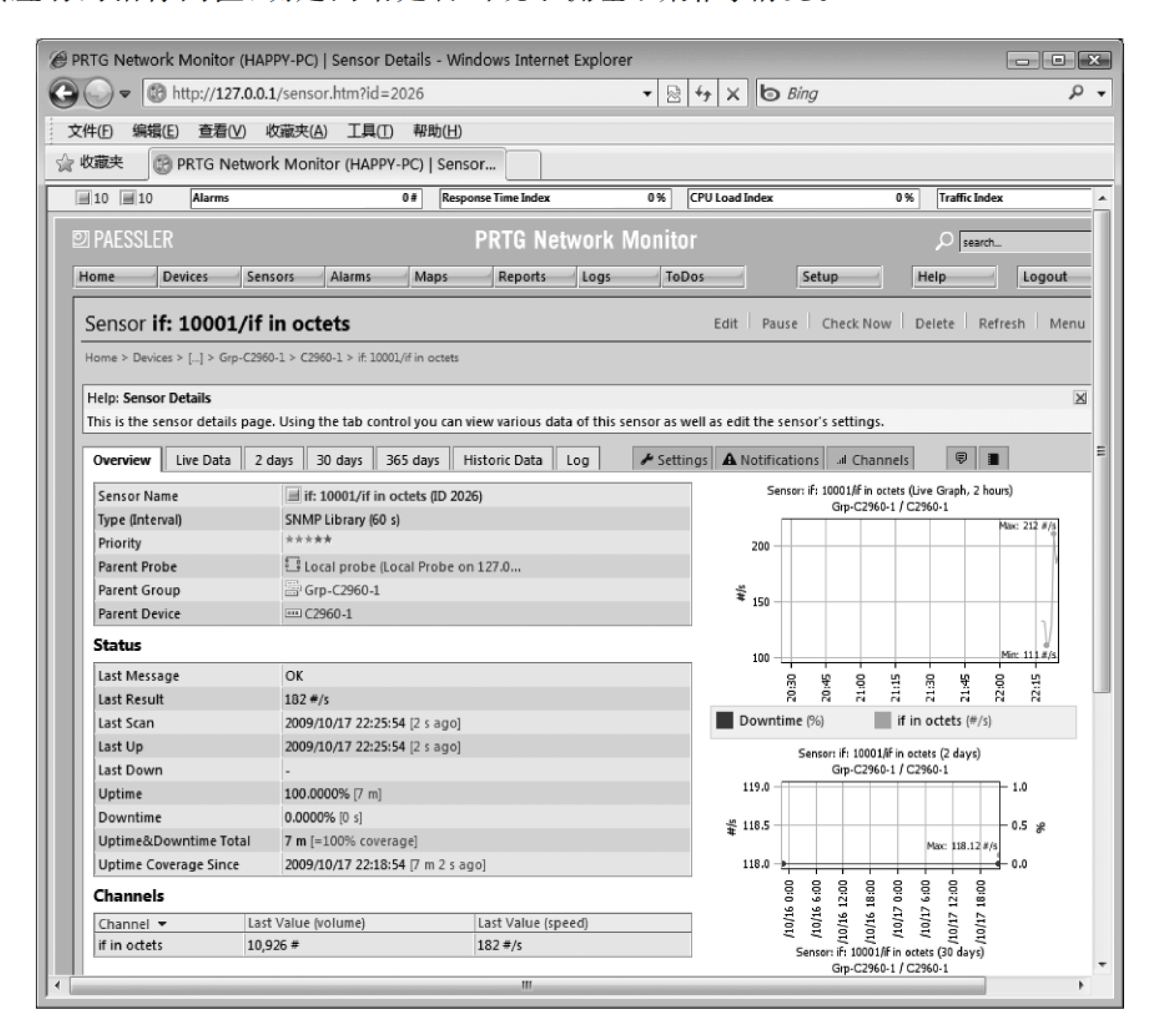


图 7-50　探测器详细信息

7.5　模拟公司网络管理实现

受到网络管理成本限制，模拟公司没有购买大型网络管理平台，而是使用了随网络设备附带的网络管理工具和一些网络上免费的网络管理软件对网络进行管理。

（1）在配置管理方面，使用 Telnet、ssh 来实现配置的修改，使用免费网络拓扑发现工具来对网络拓扑进行管理。

（2）使用 PRTG 监控、记录网络性能变化，主要包括：广域网线路各条线路的流量、广域网线路的输入/输出情况、总流量以及丢包率、错包率；并在网络设备上配置 QoS 保证网络视频会议系统的运行。

（3）在总部边界防火墙上启用入侵检测，防御来自公网的入侵。

（4）定期对公司网络进行安全审查，扫描网络设备、节点等是否存在安全风险。

（5）公司各机构网络内设置有日志服务器，用于记录网络节点上的关键事件。

7.6 小结

随着网络管理复杂度的增加,使用基于SNMP协议的网络管理平台对网络设备进行统一管理成为大中型网络管理的必然选择。本章基于模拟公司网络管理需求对网络管理的基本概念、SNMP协议的基本原理以及H3C设备和Cisco设备上网管代理的配置进行了介绍。最后简要给出模拟公司网络管理的实现方案。

7.7 习题

1. 在ISO对网络管理的定义中,网络管理的功能分为哪几个方面?
2. 典型的网络管理模型由哪几部分组成?
3. 在SNMP协议中,SNMP管理者通过什么途径从SNMP代理处获得被管对象的信息?
4. MIB的顶级对象有几个?分别是什么?
5. 在MIB树中,如何来唯一地标识一个被管对象?

7.8 实训

7.8.1 H3C网络管理配置及验证实训

实验学时:2学时。

每组实验学生人数:4人。

1. 实验目的

(1) 掌握网络设备上SNMP的配置。

(2) 掌握iMC的基本配置和使用。

2. 实验环境

(1) 安装有TCP/IP协议的Windows系统PC:4台

(2) 安装有iMC的网管工作站:1台

(3) H3C路由器:1台

(4) H3C三层交换机:1台

(5) H3C二层交换机:2台

(6) UTP电缆:9条

(7) Console电缆:4条

保持路由器和交换机均为出厂配置。

3. 实验内容

(1) 代理端配置SNMP协议。

(2) 配置并应用iMC进行网络管理。

4. 实验指导

(1) 按照图 7-51 所示的网络拓扑结构搭建网络,完成网络连接。

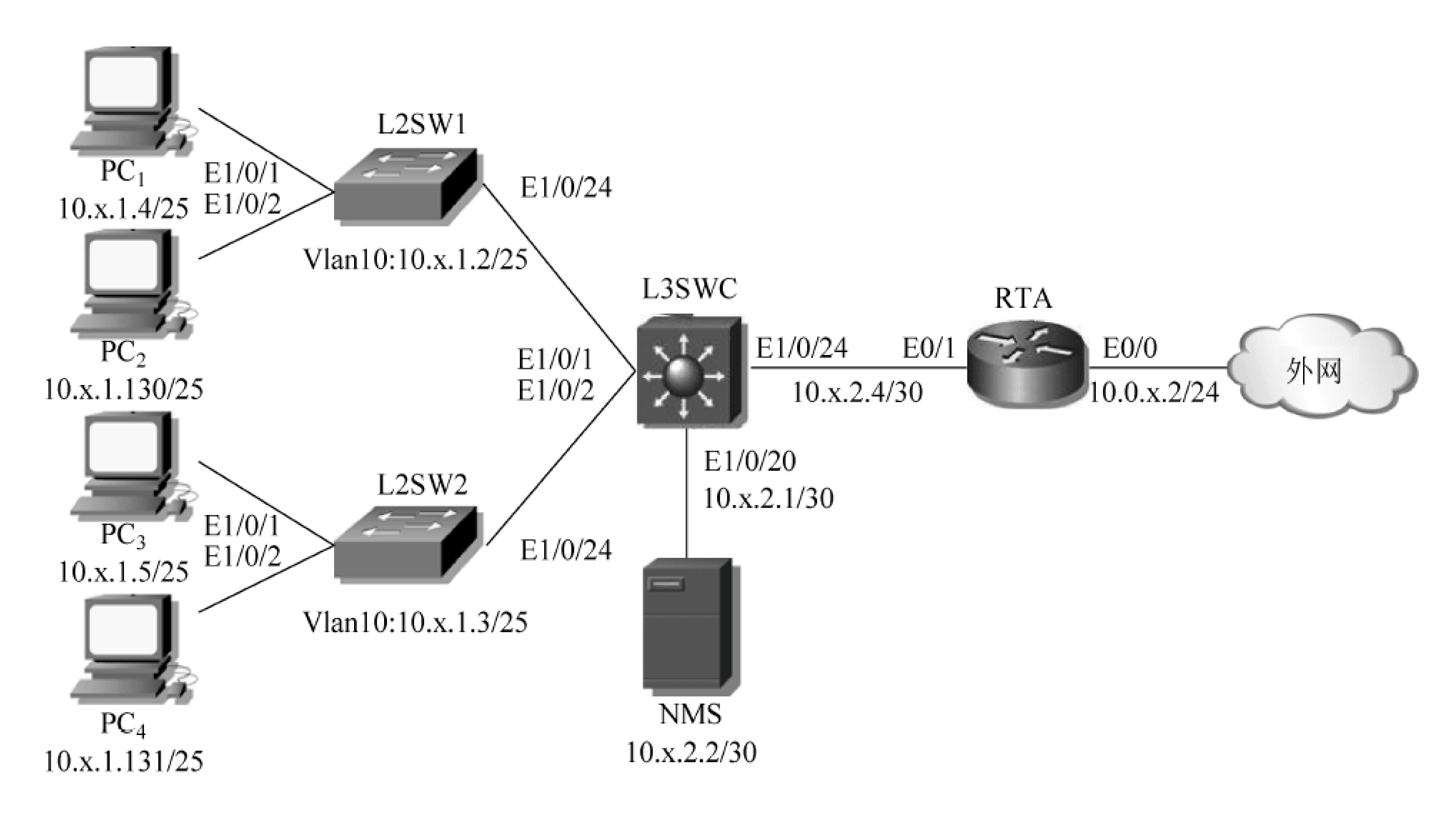


图 7-51　H3C 网络管理配置及验证实训

(2) 按照图 7-51 所示为路由器、交换机和 PC 配置 IP 地址；将 3 台交换机之间相连的链路设置为 Trunk 链路；在 3 台交换机上分别创建 VLAN 10 和 VLAN 20,在交换机 L3SW 上为三层虚接口 VLAN 10 和 VLAN 20 分别配置 IP 地址 10. x. 1. 1/25 和 10. x. 1. 129/25；在交换机 L2SW 1 和 L2SW 2 上将 E1/0/1 和 E1/0/2 分别划分到 VLAN 10 和 VLAN 20 中,配置 VLAN 10 为管理 VLAN,并为其配置图 7-31 所示的 IP 地址。在路由器 RTA 和交换机 L3SW 上配置 RIPv2,在路由器 RTA 上配置默认路由并将其引入到 RIPv2 中,保障整个网络的联通性。参考命令如下：

```
[RTA]interface Ethernet 0/1
[RTA-Ethernet0/1]ip address 10.x.2.6 30
[RTA-Ethernet0/1]quit
[RTA]interface Ethernet 0/0
[RTA-Ethernet0/0]ip address 10.0.x.2 24
[RTA-Ethernet0/0]quit
[RTA]ip route-static 0.0.0.0 0 10.0.x.1
[RTA]rip
[RTA-rip-1]version 2
[RTA-rip-1]undo summary
[RTA-rip-1]network 10.0.0.0
[RTA-rip-1]default-route originate

[L3SW]interface Ethernet 1/0/24
[L3SW-Ethernet1/0/24]port link-mode route
[L3SW-Ethernet1/0/24]ip address 10.x.2.5 30
```

```
[L3SW-Ethernet1/0/24]quit
[L3SW]interface Ethernet 1/0/20
[L3SW-Ethernet1/0/20]port link-mode route
[L3SW-Ethernet1/0/20]ip address 10.x.2.1 30
[L3SW-Ethernet1/0/20]quit
[L3SW]interface Ethernet 1/0/1
[L3SW-Ethernet1/0/1]port link-type trunk
[L3SW-Ethernet1/0/1]port trunk permit vlan all
[L3SW-Ethernet1/0/1]quit
[L3SW]interface Ethernet 1/0/2
[L3SW-Ethernet1/0/2]port link-type trunk
[L3SW-Ethernet1/0/2]port trunk permit vlan all
[L3SW-Ethernet1/0/2]quit
[L3SW]vlan 10
[L3SW-vlan10]quit
[L3SW]vlan 20
[L3SW-vlan20]quit
[L3SW]interface Vlan-interface 10
[L3SW-Vlan-interface10]ip address 10.x.1.1 25
[L3SW-Vlan-interface10]quit
[L3SW]interface Vlan-interface 20
[L3SW-Vlan-interface20]ip address 10.x.1.129 25
[L3SW-Vlan-interface20]quit
[L3SW]rip
[L3SW-rip-1]version 2
[L3SW-rip-1]undo summary
[L3SW-rip-1]network 10.0.0.0

[L2SW1]interface Ethernet 1/0/24
[L2SW1-Ethernet1/0/24]port link-type trunk
[L2SW1-Ethernet1/0/24]port trunk permit vlan all
[L2SW1-Ethernet1/0/24]quit
[L2SW1]vlan 10
[L2SW1-vlan10]port Ethernet 1/0/1
[L2SW1-vlan10]quit
[L2SW1]vlan 20
[L2SW1-vlan20]port Ethernet 1/0/2
[L2SW1-vlan20]quit
[L2SW1]management-vlan 10
[L2SW1]interface Vlan-interface 10
[L2SW1-Vlan-interface10]ip address 10.x.1.2 25
[L2SW1-Vlan-interface10]quit
[L2SW1]ip route-static 0.0.0.0 0 10.x.1.1
--------交换机 L2SW2 配置略--------
```

配置完成后,4 台 PC、NMS 和 4 台网络设备之间可以互相 ping 通,并且均可以连接外部网络。

(3) 在 4 台网络设备上进行 SNMP 的配置,使其可以被网管工作站 NMS 上的 iMC 管理。其中只读团体名为 GZ08*tK,读写团体名为 RS30#tL。参考命令如下:

```
[RTA]snmp-agent
[RTA]snmp-agent sys-info version all
[RTA]snmp-agent community read GZ08*tK
[RTA]snmp-agent community write RS30#tL
[RTA]snmp-agent trap enable
[RTA]snmp-agent target-host trap address udp-domain 10.x.2.2 params securityname GZ08*tK
--------交换机 L3SW、L2SW1 和 L2SW2 配置略--------
```

(4) 在 NMS 上启动并登录 iMC,首先进行自动发现,自动发现配置如图 7-52 所示。

自动发现(简易)	上次发现结果　切换到高级模式　设置缺省监视指标
网段设置(必须)	
开始IP	
结束IP	增加
* 已设置的网段地址	10.x.1.1-10.x.1.131 10.x.2.1-10.x.2.6　删除
设备分组	
SNMP & Telnet 参数设置	
* SNMP读团体字	GZ08*tK
* SNMP写团体字	RS30#tL
* Telnet认证模式	无用户名 +无密码
定时发现设置	
* 定时发现方式	从不
仅保存设置	自动发现

图 7-52 自动发现配置

注意:在配置自动发现的网段时,切勿配置其他台席上的网段,否则会发现并管理其他台席上的设备,造成不同实验台席之间管理上的混乱。

自动发现完成后,在"资源"标签下单击"网络拓扑视图"进入"拓扑"页面,在"拓扑"页面下双击"我的网络拓扑",查看 iMC 发现的网络拓扑;双击"IP 拓扑",查看 iMC 发现的 IP 拓扑,比较两个拓扑之间的异同。在"我的网络拓扑"界面下双击某一条链路查看该链路的基本信息和链路两端接口的详细信息。在"我的网络拓扑"界面下右击某一台设备并在弹出的菜单中选择"打开设备面板",查看相应设备的物理运行情况。在"我的网络拓扑"界面下右击某一台设备并在弹出的菜单中选择"同步",同时在 NMS 上打开 Wireshark 软件捕获 SNMP 数据报文,查看 NMS 与相应设备之间的交互过程。

在设备之间人为制造大的数据流量,例如持续不断的大长度的 ping 报文,然后在设备的具体管理界面查看性能监视信息。在设备具体管理界面右侧的"性能监视"栏中单击"查看性能数据",查看相应设备在某一时间段中的内存利用率、设备不可达性比例、CPU 利用率以及设备响应时间等性能监控数据信息。在"资源"标签左下角的"性能管理"栏中单击"TopN" 查看某一时间段中的性能统计信息排序列表。

将某台 PC 与交换机之间的物理连接人为断开,然后再恢复连接,在"告警"界面查看相应的告警信息,并在 NMS 上打开 Wireshark 软件捕获 SNMP 数据报文,查看从交换机

发送给 NMS 的 Trap 报文。

在网络设备上配置 Telnet 服务,在 iMC 上配置 Telnet 模板,在设备的具体管理界面右侧的"配置"栏中单击"修改 Telnet 参数",并在弹出"Telnet 参数设置"对话框中选择相应的模板,在设备的具体管理界面右侧的"动作"栏中单击"Telnet"远程登录到设备上进行配置和管理。

5. 实验报告

<table>
<tr><td rowspan="4">SNMP 的配置</td><td>RTA</td><td colspan="8"></td></tr>
<tr><td>L3SW</td><td colspan="8"></td></tr>
<tr><td>L2SW1</td><td colspan="8"></td></tr>
<tr><td>L2SW2</td><td colspan="8"></td></tr>
<tr><td rowspan="9">iMC</td><td>自动发现网段设置</td><td colspan="8"></td></tr>
<tr><td rowspan="4">网络拓扑操作</td><td rowspan="2">RTA-L3SW 链路信息</td><td colspan="2">连接类型</td><td>左节点</td><td colspan="2">左接口描述</td><td>右节点</td><td>右接口描述</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="2">L2SW1 面板情况</td><td colspan="4">处于 UP 状态的端口</td><td colspan="3">处于 DOWN 状态的端口</td></tr>
<tr><td colspan="4"></td><td colspan="3"></td></tr>
<tr><td>内存利用率 TopN 排序</td><td colspan="8"></td></tr>
<tr><td rowspan="3">告警管理</td><td colspan="2"></td><td colspan="4">告警名称</td><td colspan="2">告警级别</td></tr>
<tr><td colspan="2">断开连接</td><td colspan="4"></td><td colspan="2"></td></tr>
<tr><td colspan="2">恢复连接</td><td colspan="4"></td><td colspan="2"></td></tr>
</table>

7.8.2 Cisco 网络管理配置及验证实训

实验学时:2 学时。

每组实验学生人数:4 人。

1. 实验目的

(1) 掌握网络设备上 SNMP 的配置。

(2) 掌握故障排查定位方法。

(3) 掌握防火墙上配置入侵检测与防御的操作方法。

(4) 掌握网络设备记录日志的配置方法。

(5) 掌握使用 PRTG 监控网络性能的方法。

2. 实验环境

(1) 安装有 TCP/IP 协议的 Windows 系统 PC:3 台

(2) Cisco 路由器:1 台

(3) Cisco PIX 防火墙:1 台

(4) UTP 交叉电缆:4 条

(5) Console 电缆:2 条

保持路由器和防火墙均为出厂配置。

3. 实验内容

(1) 记录日志配置。

(2) 入侵检测配置。

(3) 性能管理配置。

4. 实验指导

(1) 按照图 7-53 所示的网络拓扑结构搭建网络,完成网络连接。

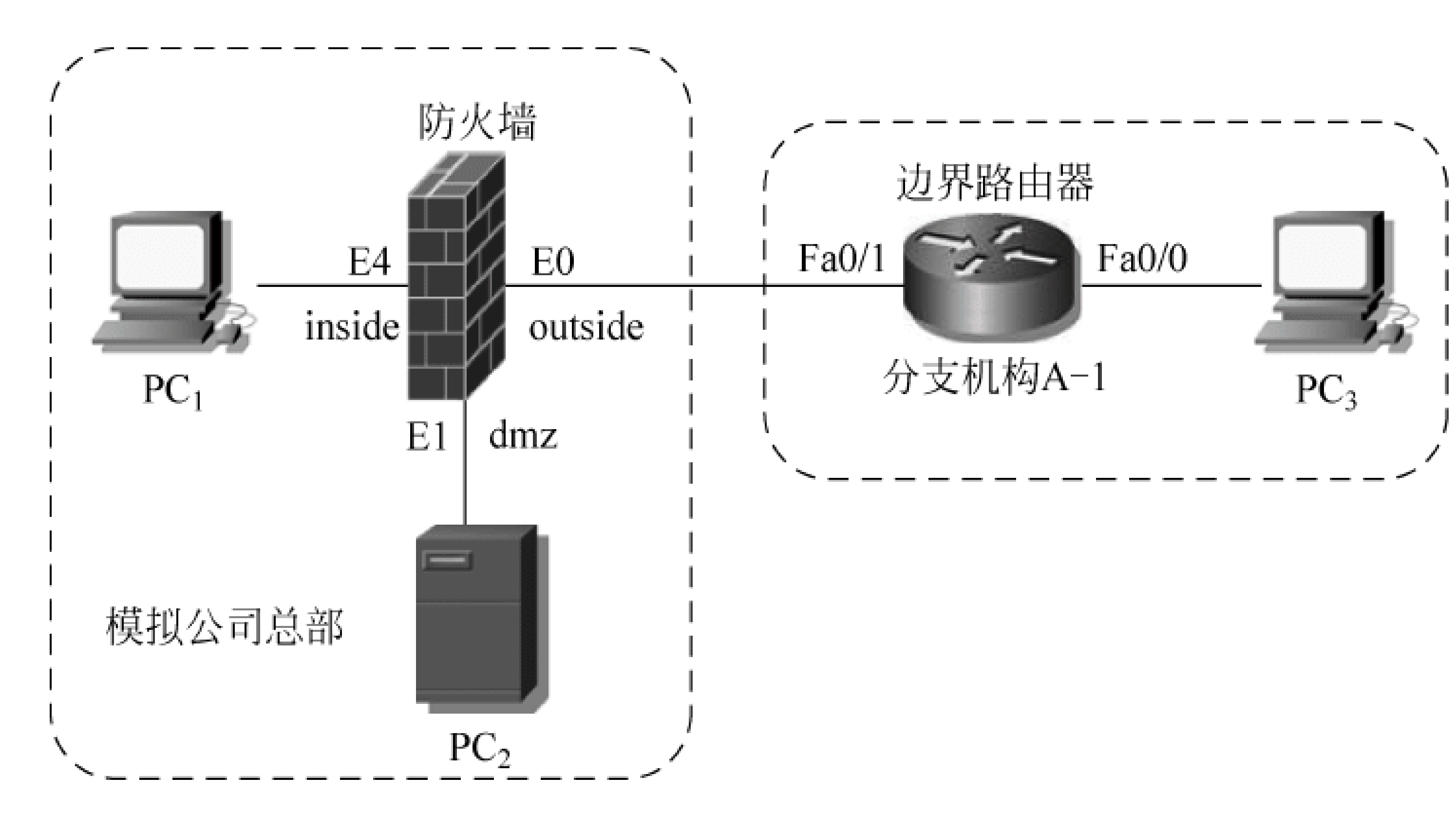


图 7-53 Cisco 网络管理配置及验证实训

该网络中 IP 地址分配如表 7-5 所示。其中 PC_1 和 PC_3 用于分别模拟各自网络中的日志服务器以及主机。在实训开始前按表 7-5 配置好网络连接和路由。

表 7-5 网络管理实训地址分配

接 口	IP 地址/网络前缀	网 关
PC_1(模拟内网主机、日志服务器)	200.100.8.122/30	200.100.8.121/30
PC_2(模拟 FTP 服务器)	200.100.8.28/27	200.100.8.30/27
PC_3(模拟外网主机、日志服务器)	200.100.15.198/30	200.100.8.121/30
防火墙 e0 接口(outside)	200.100.8.126/30	—
防火墙 e1 接口(dmz)	200.100.8.30/27	—
防火墙 e4 接口(inside)	200.100.8.121/30	—
路由器 fa0/0	200.100.8.125/30	—
路由器 fa0/1	200.100.15.197/30	—

(2) 配置网络设备 Telnet 访问许可,并使用 Telnet 对设备进行远程管理。在分支机构边界路由器和总部防火墙上分别配置 Telnet 访问许可,并使用 PC_1、PC_2、PC_3 登录各网络设备,测试能否对网络设备进行配置。

在分支机构边界路由器的参考配置操作如下:

```
a1(config)#enable secret 123
a1(config)#line vty 0 4
a1(config-line)#password 123
a1(config-line)#login
```

在总部防火墙参考配置操作如下:

```
zbfw(config)# telnet 200.100.8.122 255.255.255.255 inside
zbfw(config)# passwd 123
zbfw(config)# enable password 123
```

(3) 为网络设备记录日志。启用分支机构边界路由器和总部防火墙上的日志记录功能。分别在 PC_1、PC_3 上启动 syslog 服务器记录日志信息。

在分支机构边界路由器的参考配置操作如下:

```
a1(config)#logging on
a1(config)#logging host 200.100.15.198
a1(config)# logging trap informational
```

在总部防火墙上参考配置操作如下:

```
zbfw(config)# logging enable
zbfw(config)# logging host inside 200.100.8.122
zbfw(config)# logging trap informational
```

有关日志服务器配置请参考7.4.2小节。

(4) 网络入侵检测配置。在总部防火墙上配置入侵检测与防御,并分别在 PC_1、PC_2、PC_3 上运行攻击软件,攻击对方网络中的主机。检查防火墙的入侵检测与防御是否起到作用。

在总部防火墙上配置入侵检测与防御参考配置操作如下:

```
zbfw (config)#ip audit name attids attack action alarm reset
zbfw (config)#ip audit name inforids info action alarm
zbfw (config)#ip audit interface outside attids
zbfw (config)#ip audit interface dmz inforids
zbfw (config)#ip audit interface inside inforids
```

(5) 使用 PRTG 监控网络性能。

在分支机构边界路由器和总部防火墙上配置 SNMP 代理,在 PC_2、PC_3 上运行 PRTG 监控路由器和防火墙的接口流量变化。在 PC_1 上使用浏览器从 PC_2、PC_3 上使用 FTP 下载大文件,观察网络设备接口流量信息的变化。

在分支机构边界路由器的参考配置操作如下:

```
a1 (config)#snmp-server community a1-pub
a1(config)#snmp-server host inside 200.100.15.198 a1-pub
a1(config)# snmp-server enable traps
```

在总部防火墙上参考配置操作如下:

```
zbfw (config)#snmp-server community zb-pub
zbfw (config)#snmp-server host inside 200.100.8.122 zb-pub
zbfw(config)# snmp-server enable traps
```

有关 PRTG 配置请参考7.4.2小节。

(6) 故障排查定位。

通过网络攻击、物理破坏、错误配置等方式,分别设置网络服务、网络路由、网络链路、网络线路 4 种故障,提供给学生进行排查。

5. 实验报告

---

1. 根据实验指导配置

能在 PC_3 上使用 Telnet 远程登录到防火墙吗? 能□ 不能□,为什么? ________________________

能在 PC_2 上使用 Telnet 远程登录到防火墙吗? 能□ 不能□,为什么? ________________________

---

2. 在配置完日志记录后,分别在 PC_1、PC_2、PC_3 上使用网络攻击软件发动攻击,记录在日志服务器上的相应记录。

PC_1 攻击 PC_2 时的日志记录:

PC_2 攻击 PC_3 时的日志记录:

PC_3 攻击 PC_1 时的日志记录:

---

3. 在配置完日志记录和入侵检测后,分别在 PC_1、PC_2、PC_3 上使用网络攻击软件发动攻击,记录在日志服务器上的相应记录。

PC_1 攻击 PC_2 时的日志记录:

PC_2 攻击 PC_3 时的日志记录:

PC_3 攻击 PC_1 时的日志记录:

---

4. 在路由器和防火墙上配置 SNMP 代理,并在 PC_1、PC_3 上配置 PRTG,监测并记录路由器和防火墙的接口流量信息。

路由器接口 fa0/1 上的入站流量:平均值____________最大值____________

防火墙接口 inside 上的入站流量:平均值____________最大值____________

防火墙接口 outside 上的入站流量:平均值____________最大值____________

防火墙接口 dmz 上的入站流量:平均值____________最大值____________

---

5. 在 PC_2 上运行网络攻击软件,并在 PC_1、PC_3 上分别从对方服务器上使用 FTP 服务下载大文件,监测并记录路由器和防火墙的接口流量信息。

路由器接口 fa0/1 上的入站流量:平均值____________最大值____________

防火墙接口 inside 上的入站流量:平均值____________最大值____________

防火墙接口 outside 上的入站流量:平均值____________最大值____________

防火墙接口 dmz 上的入站流量:平均值____________最大值____________

附录 A

习题参考答案

第 1 章

1. 网络安全从本质上讲就是网络上的信息安全，是指网络系统的硬件、软件以及系统中的数据受到保护，不受偶然的或者恶意的因素而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科，因此称其为一门综合性的学科。

2. 扫描攻击可以分为 IP 地址扫描和端口扫描两种形式，其中 IP 地址扫描的目的是发现网络中存活的 IP 地址；端口扫描的目的是探测目标主机的哪些端口处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。

3. 会话劫持攻击是指在一次正常的会话过程当中，攻击者作为第三方参与到其中，它可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。按照攻击方式可以将会话劫持攻击分为主动劫持和被动劫持两种。

4. 拒绝服务攻击是通过向网络中的网络设备、计算机等发送大量消耗、占用其资源的流量，使被攻击网络或主机无法及时接收并处理外界请求，从而导致无法提供正常网络服务的攻击方式。

典型的拒绝服务攻击有 SYN 洪水攻击、死亡之 ping 攻击和泪滴攻击等。

5. 在分布式拒绝服务攻击的体系结构中共有 4 种不同的角色：

(1) 攻击者作为 DDoS 攻击中的主控台，负责向主控端发送攻击命令。

(2) 主控端负责接收来自攻击者的攻击命令并将其发送到代理端来控制代理端的攻击。

(3) 代理端负责接收并运行主控端发来的攻击命令，对被攻击者实施攻击。

(4) 被攻击者是攻击的受害者，一般多为一些对外提供访问服务的网站、邮件服务器以及数据库系统等。

第 2 章

1. 规则中的 IP 地址为 202.207.120.0，由于 IP 地址中的第 23 位不需要进行匹配，因此通配符掩码为 0.0.2.255。

2. 因为不同品牌的设备在对 ACL 默认规则的处理上可能不同，而且默认规则的动作可以通过命令来修改，从而可能造成同一品牌设备的默认规则也不同。为了保证 ACL 的健壮性和可移植性，一般应将所有的规则显式地写出，而尽量避免使用 ACL 的默认规则。

3. ACL 的应用位置应该在不影响其他合法流量的前提下尽可能靠近被拒绝的源。但实际上，基本 ACL 应放在离数据报文的目的地尽可能近的地方；高级 ACL 应放在离数据报文源地址尽可能近的地方。

4. 之所以不需要指定对 20 端口的访问允许，是因为当 FTP 工作在被动模式下，FTP 服务器使用的数据端口为大于 1024 的随机端口而非 20 端口；而当 FTP 工作在主动模式下，由于是由 FTP 服务器主动发起数据连接，因此返回的数据流量可以使用携带参数 established 的规则匹配，而没有必要专门指定一条对 20 端口访问允许的规则。

5. 不能使用 detect tcp 来代替 detect ftp，因为 FTP 是一个多通道的应用层协议，如果直接使用 TCP 进行检测可能会导致无法建立 FTP 的数据连接。

第 3 章

1. 内部网络地址转换共有 5 种不同的类型，分别是静态网络地址转换、动态网络地址转换、网络地址端口转换、基于接口的地址转换和端口地址重定向。

2. C

3. A

4. 在 H3C 设备上，当在同一个接口上 ACL 和 NAT 共存时，ACL 应对内部本地地址进行约束，这取决于设备对 NAT 和 ACL 的处理顺序。在 H3C 的设备上，对出站流量先去匹配出站 ACL，然后再进行 NAT；对入站流量先进行 NAT，然后再去匹配入站 ACL。

第 4 章

1. 按照加密算法工作方式的不同，可以将加密技术分成对称加密技术和非对称加密技术两种，其中典型的对称加密算法有 DES、3DES 和 AES 算法；典型的非对称加密算法有 RSA 和 D-H 算法。

2. 散列算法具有一些特点：

(1) 对同一源数据反复进行散列运算得出的散列结果总是相同；

(2) 对源数据的一个细小的修改都会导致产生完全不同的散列值；

(3) 由于在散列的过程中损失了信息，因此散列具有不可逆性，即无法通过生成的散列值计算出源数据。

3. ESP 协议既可以对数据进行加密，也可以对数据的完整性进行验证；AH 协议不提供加密功能，但 AH 协议的数据完整性验证功能要比 ESP 的强。

4. IKE 协商可以分为两个阶段，分别是协商建立 ISAKMP SA 和协商建立 IPSec SA，其中第一个阶段的协商有两种工作模式，分别是主模式和野蛮模式。

5. L2TP 隧道的建立包括 NAS 发起和客户端发起两种模式，其中 NAS 发起模式中由 LAC 端发起 L2TP 隧道的连接；客户端发起模式中由支持 L2TP 协议的远程用户发

起 L2TP 隧道的连接。

第 5 章

1. 按照实现方式的区别,防火墙可以被分为3种类型,分别是基于服务器的防火墙、集成防火墙和基于设备的防火墙。

2. 在 H3C 的防火墙上,共有5安全区域,分别是:内部区域,安全级别为85;外部区域,安全级别为5;DMZ 区域,安全级别为50;Management 区域,安全级别为100;Local 区域,安全级别为100。

3. 在 H3C 的防火墙上,默认高安全级别的区域能够访问低安全级别的区域,低安全级别的区域不能访问高安全级别的区域。但所有的区域均可访问 Local 区域,以保证无论主机处于哪一个区域均可以保持与防火墙本身的联通性。

4. 防火墙有三种不同的工作模式,分别是:透明模式,适用于在已有的网络中增加的防火墙设备;路由模式,适用于在新建网络中作为网络接入设备的防火墙;混合模式,适用于网络要求其某些接口工作在二层,某些接口工作在三层的防火墙设备。

5. 统一威胁管理设备是由硬件、软件和网络技术组成的具有专门用途的设备,它主要提供一项或多项安全功能,同时将多种安全特性集成于一个硬件设备里,形成标准的统一威胁管理平台。UTM 在提供传统防火墙、VPN 功能基础上,一般还提供病毒防护、URL 过滤、漏洞攻击防护、垃圾邮件防护、P2P/IM 应用层流量控制和用户行为审计等安全功能。由于 UTM 设备综合了多项安全功能并且易于管理,目前正逐渐代替传统的防火墙成为主流的信息安全产品。

第 6 章

1. AAA 技术中的3个A分别代表认证(Authentication)、授权(Authorization)和计费(Accounting)。

2. D

3. 受控端口和非受控端口是一个物理端口上的两个逻辑端口。受控端口只有在授权状态下才会处于联通状态,用于传递业务报文;非受控端口始终处于双向联通状态,用于传递 EAPOL 协议帧。

4. PAE 是端口访问实体,其中设备端 PAE 利用认证服务器对需要接入局域网的客户端进行认证,并根据认证结果来控制受控端口的状态为授权或者非授权;客户端 PAE 负责响应设备端的认证请求,向设备端提交用户的认证信息,也可以主动向设备端发送认证请求和下线请求。

5. EAP 信息在 RADIUS 报文中的承载 EAP 中继和 EAP 终结两种方式,其中在 EAP 中继方式中设备端 PAE 将完整的 EAP 报文直接封装在 RADIUS 报文中传递给认证服务器;在 EAP 终结方式中 EAP 协议报文在设备端被终结,设备端 PAE 将 EAP 报文中的有用参数信息放置在 RADIUS 报文中的 PAP 或 CHAP 属性参数中传递给认证服务器。

6. Intrusion Protection 特性的作用是在端口收到源 MAC 地址为非法 MAC 的数据

帧时，对端口采取相应的安全策略以确保端口的安全性。

7. 端口绑定的目的是使交换机只对从相应端口收到的指定 IP 地址和指定 MAC 地址的数据报文进行转发，从而实现对端口转发的报文进行过滤控制，增强端口的安全性，实现 IPSG 的功能。

8. 在 DHCP Snooping 中，系统通过监听 DHCP-REQUEST 报文和从信任端口上收到的 DHCP-ACK 报文，来获取相应端口上连接的客户端的 MAC 地址和 IP 地址信息，实现动态绑定。

9. 在 EAD 中，联动设备一般是交换机、路由器、VPN 网关或无线设备等网络设备。作为网络中安全策略的实施点，联动设备起到强制用户准入认证、隔离不合格终端和为合法用户提供网络服务的作用。

第 7 章

1. 在 ISO 对网络管理的定义中，网络管理的功能分为故障管理、配置管理、计费管理、性能管理和安全管理 5 个方面。

2. 典型的网络管理模型由 4 部分组成，分别是：网络管理实体、网络管理代理、网络管理协议和管理信息库。

3. 在 SNMP 协议中，SNMP 管理者从 SNMP 代理获得被管对象信息的途径有两种：轮询和自陷。轮询是指 SNMP 管理者周期性地向网络中的各个 SNMP 代理发送查询命令来获得被管设备上各个被管对象的数据信息；自陷是指在网络中出现了异常事件的时候，相应的 SNMP 代理主动向 SNMP 管理者发送陷阱报文。

4. MIB 的顶级对象有 3 个，分别是代表国际电信联盟远程通信标准化组织的 ccitt、代表国际标准化组织的 iso 和这两个组织的联合体 joint-iso-ccitt。

5. 在 MIB 树中，被管对象使用从根开始的一条路径来唯一地识别，这条用数字串来表示的路径称为被管对象的对象标识符。

附录 B

利用模拟器 GNS3 搭建模拟实训环境

由于使用真实网络设备进行实训成本较高，所以使用网络模拟器软件模拟网络设备进行网络实验就成为一种比较经济的替代方案。目前常见模拟 Cisco 网络设备的模拟器软件有思科网络学院的 PacketTracer、Routersim、Boson 实验模拟器和免费的 Dynamips、Pemu、GNS3 等。

GNS3（http://www.gns3.net/）是一款图形化的网络模拟器。它集成了模拟路由器的 Dynamips 和模拟 Cisco PIX 防火墙的 Pemu 模拟器软件，可以使用图形化界面搭建网络模拟环境。Dynamips、Pemu 的优点是直接使用 Cisco 网络设备的 IOS 映像文件进行模拟，操作更真实。

GNS3 可以模拟路由器、防火墙，但对 PC 和交换机的模拟功能较差。

如果实训环境需要多台 PC，则可以安装虚拟 PC 模拟器来辅助 GNS3 解决问题。Virtual PC Simulator 软件是一款开源 PC 模拟软件，可以模拟 9 台虚拟 PC，并支持对这些 PC 配置 IP、运行 ping、traceroute 命令等。通过虚拟 PC 模拟器 Virtual PC Simulator 与 GNS3 的 cloud 图标结合可以实现在 GNS3 中模拟多台虚拟 PC。

GNS3 中不支持交换机的模拟，但可以使用带交换模块的 3700、3600 系列路由器来模拟部分交换机功能。

B.1 安装并配置 GNS3 初始环境

B.1.1 安装 GNS3

安装 GNS3 的操作非常简单，首先从 GNS3 官方网站“http://www.gns3.net/download”下载 GNS3 模拟器软件，例如“GNS3-0.6.1-win32-all-in-one.exe”；然后打开 Windows 资源管理器，找到下载的 GNS3 模拟器软件，双击进行安装。GNS3 需要 winpcap 支持，所以安装过程中，会提问是否安装该软件，按照默认选项安装即可。

注意：GNS3 不支持中文目录名、文件名处理。所以一定将 GNS3 所有工作目录、相关文件名设置为英文。

B.1.2 配置 GNS3 初始环境

GNS3 安装后需要重新启动操作系统，才能正常运行。

1. GNS3 初始配置窗口

GNS3 启动后会出现图 B-1 所示初始配置提示窗口。该窗口提示要使用 GNS3，需要完成两步操作：第 1 步，配置 GNS3 运行参数；第 2 步，导入网络设备 IOS。单击[1]按钮，进入 GNS3 运行参数配置，单击[2]进入导入网络设备 IOS 操作。

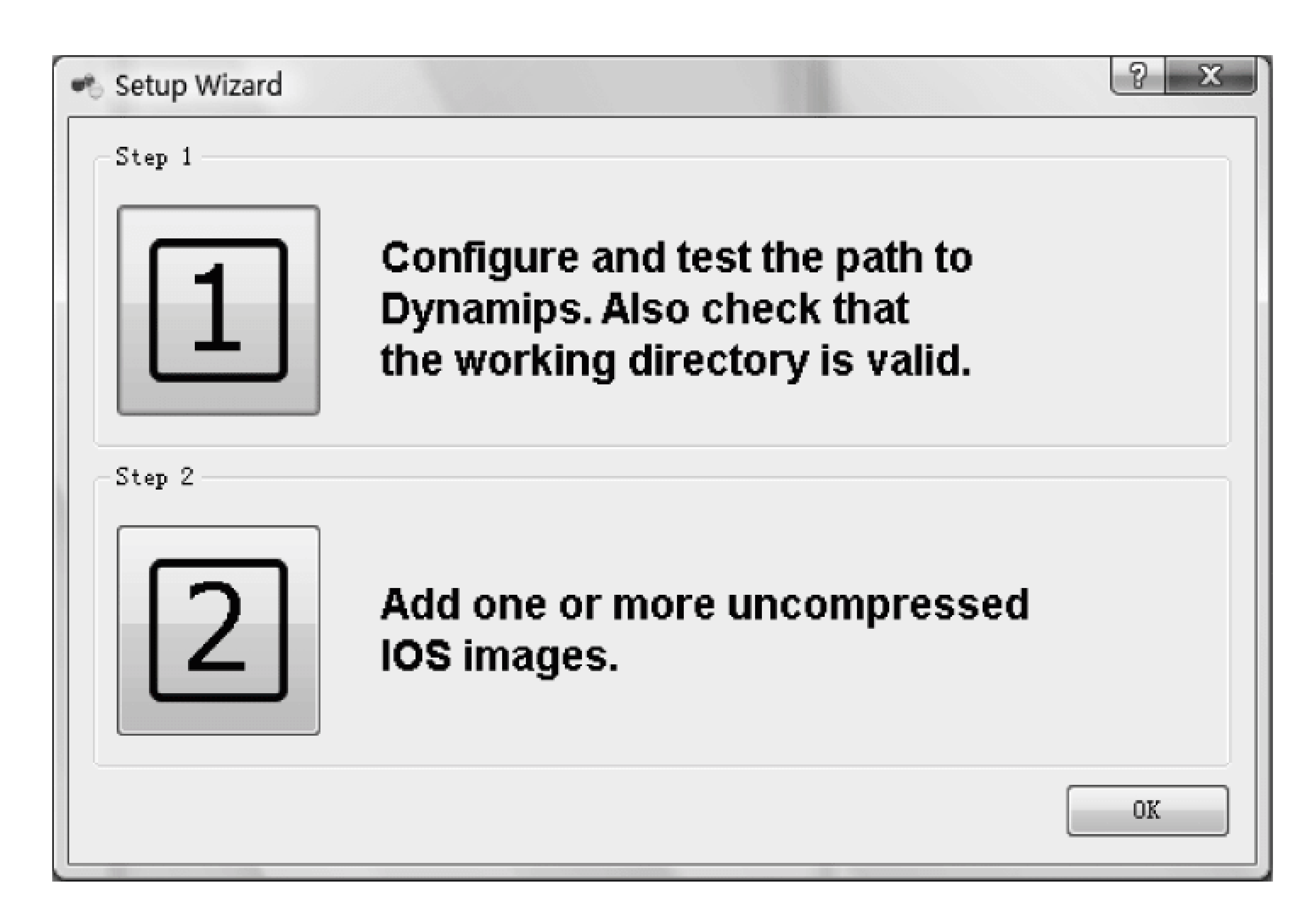


图 B-1 GNS3 初始配置窗口

2. 配置 Dynamips、Pemu 等运行环境参数

如前所述，GNS3 结合了 Dynamips、Pemu 等软件功能，所以在安装 GNS3 后需要配置 Dynamips、Pemu 等运行环境参数。在图 A-1 所示初始配置窗口单击[1]按钮，或在 GNS3 主窗口中选择"Edit|Preferences"命令，都可以进行 GNS3 运行参数配置。

如图 B-2 所示，GNS3 运行参数配置包括四部分：一般配置、Dynamips 配置、Pemu 配置和 Capture 配置。

在 GNS3 一般配置中，可以选择软件"语言"为"简体中文"，以便于使用。

另外，需要选择连接到模拟网络设备的终端程序。在 GNS3 首选项窗口，单击窗口左边列表框中的"一般"选项，在右边"终端命令"文本框中输入"C:\Program Files\Putty\putty. exe -telnet %h %p"，让 GNS3 模拟器调用 Putty 软件访问虚拟网络设备，从而可以在终端窗口中对虚拟网络设备进行配置。当然，Putty 软件需要提前安装好。

在 Pemu 配置中，需要为 Cisco PIX 防火墙配置默认 IOS 映像文件、序列号和 Key，如图 B-3 所示。

Dynamips 和 Capture 运行环境可以使用默认配置，不用更改。

3. 添加各网络设备 IOS 映像文件

在 GNS3 初始窗口，单击[2]按钮，或者选择"编辑—IOS 和 Hypervisors"命令，都可以

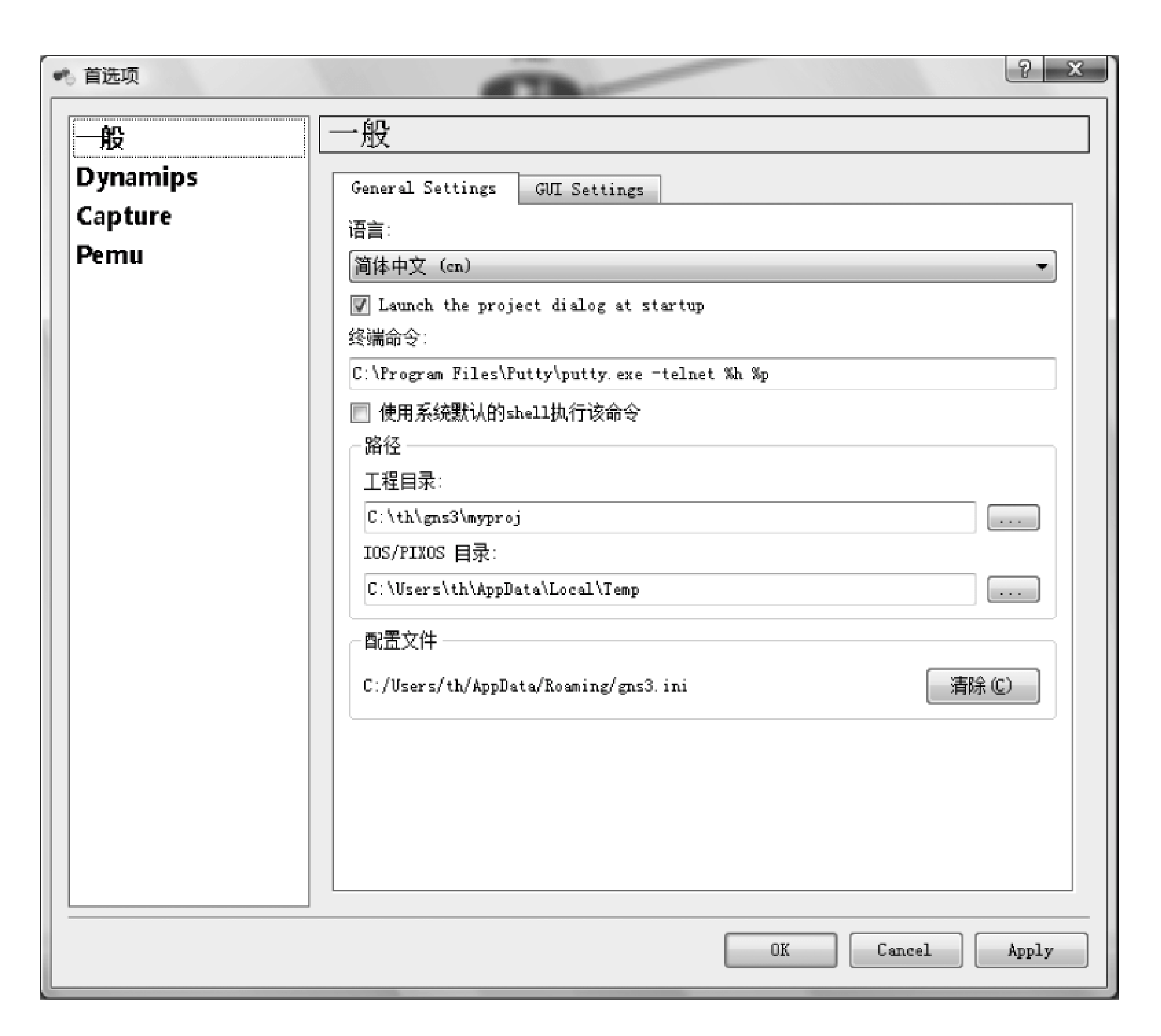


图 B-2　GNS3 运行环境参数配置窗口

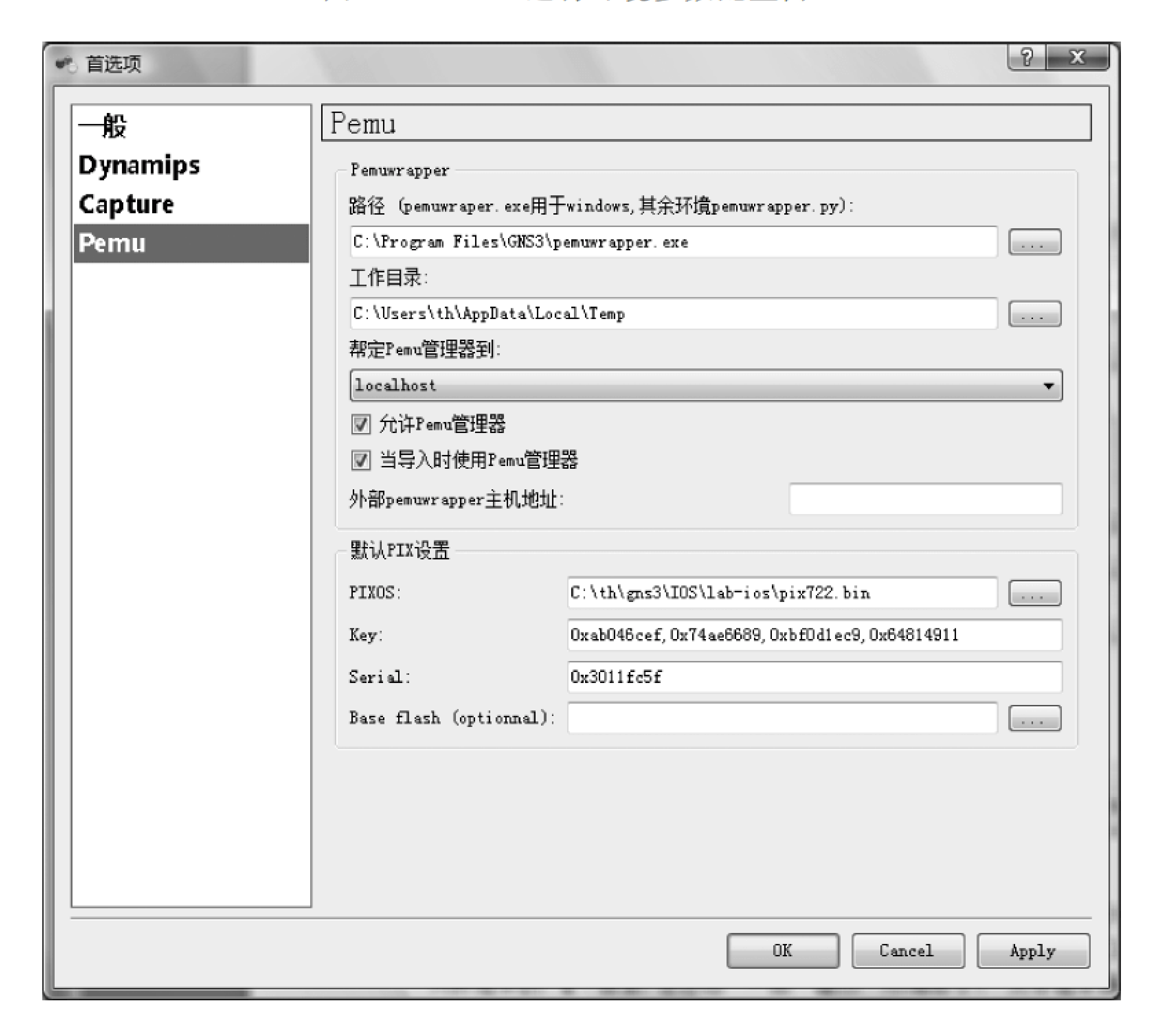


图 B-3　Pemu 运行环境配置窗口

打开图 B-4 所示“IOS 映像文件及 Hypervisors 管理窗口”，为实验模拟的网络设备导入所需的 IOS 映像文件。

图 B-4　导入 IOS 映像文件窗口

在图 B-4 中“平台”下拉列表框中，选择需要配置的设备系列号。在“型号”下拉列表框中，选择需要配置的设备型号。单击“IOS 文件”文本框右边的 ... 按钮，找到并选中相应的 IOS 映像文件，单击“打开”按钮确定返回，为所选设备配置 IOS 映像文件。

单击窗口左下方的 保存(S) 按钮，保存配置。此时在窗口上方的 IOS 列表框中会出现所配置的 IOS 映像文件。

B.2　使用 GNS3 模拟网络设备进行实验

使用 GNS3 模拟网络设备的操作非常简单。

在图 B-5 所示主窗口中，用鼠标拖曳左边的网络设备图标到中间窗口，然后右击网络设备，在弹出菜单中选择▶开始命令，启动设备。

单击 GNS3 窗口快捷栏上的按钮，在弹出窗口中选择连接线缆类型，如图 B-6 所示。此时按钮的图标变为，鼠标变为十字形。用鼠标分别单击要连接的两个网络设备，可以将网络设备连接起来。

单击图 B-5 所示 GNS3 主窗口中的图标，打开网络设备终端窗口，即可对网络设备进行配置。

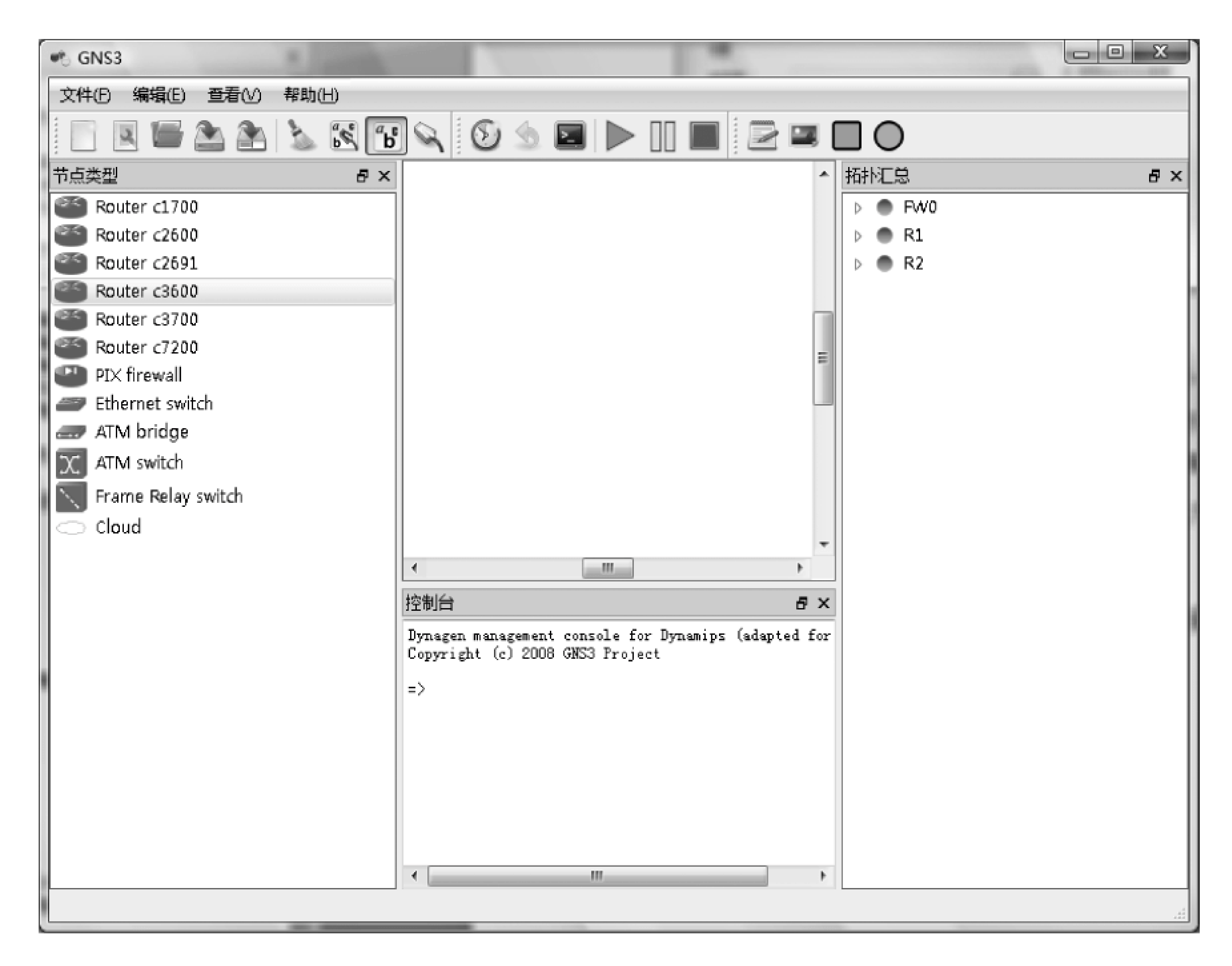


图 B-5 GNS3 主窗口

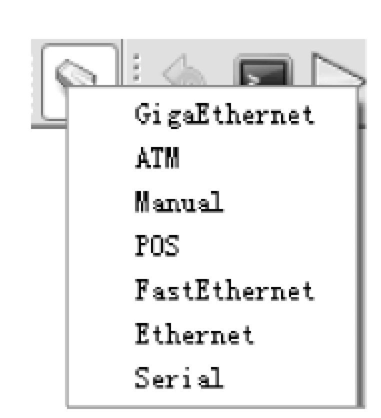


图 B-6 连接线缆类型菜单

附录 C

iMC 安装指导

H3C 的智能管理中心可以安装在 Windows、Linux 或 Solaris 操作系统中运行，在 Windows 环境下使用 SQL Server 数据库、在 Linux 或 Solaris 环境中使用 Oracle 数据库来实现网络管理数据的存储和管理。在本附录中以 Windows 环境下 iMC 的安装为例进行介绍。

C.1 iMC 安装环境要求

C.1.1 iMC 安装硬件环境要求

一般网络管理软件对计算机的硬件环境要求都比较高，因此基本上都会采用专门的服务器或者高配置的计算机来作为网管工作站。iMC 对计算机硬件的最低配置要求如表 C-1 所示。

表 C-1 iMC 安装硬件环境要求

硬件名称	配置要求	硬件名称	配置要求
CPU	主频≥3.0GHz	硬盘	≥144GB
内存	≥2GB	网卡	100/1000Mb 自适应

C.1.2 iMC 安装软件环境要求

iMC 对计算机上已安装软件的要求如表 C-2 所示。

表 C-2 iMC 安装软件环境要求

软件名称	安装要求
操作系统	Windows Server 2003/2008 或 Windows XP Professional Windows Server 2003 需要安装 Service Pack 2 补丁
数据库	Microsoft SQL Server 2005/2008 SQL Server 2005 需要安装 Service Pack 2 补丁

C.2　iMC的安装过程

iMC包括智能管理平台和业务组件两部分,其中智能管理平台为必配组件,包括了资源管理、ACL管理、网元管理、性能管理以及告警管理等公共组件;业务组件包括用户接入管理、EAD安全策略组件以及无线业务管理等,业务组件可以由用户根据业务需求进行选配。

智能管理平台是实现多种业务的基础,在安装时必须先安装智能管理平台,然后才能安装各个业务组件。本部分只对智能管理平台的安装进行介绍。

首先,将iMC智能管理平台的安装光盘放入光驱,进入光盘目录下的“windows\install”目录,运行该目录下的install.bat文件,弹出如图C-1所示的对话框。

在图C-1所示的对话框中选择“国家/地区”和“语言”,然后单击“确定”按钮,H3C智能管理中心安装向导开始进行安装环境的检查工作,安装向导会对计算机的端口占用情况、物理内存大小以及SQL Server数据库的安装情况进行检查,如果安装环境不符合要求,则iMC将无法安装。其中检查数据库连接部分会弹出如图C-2所示的对话框。

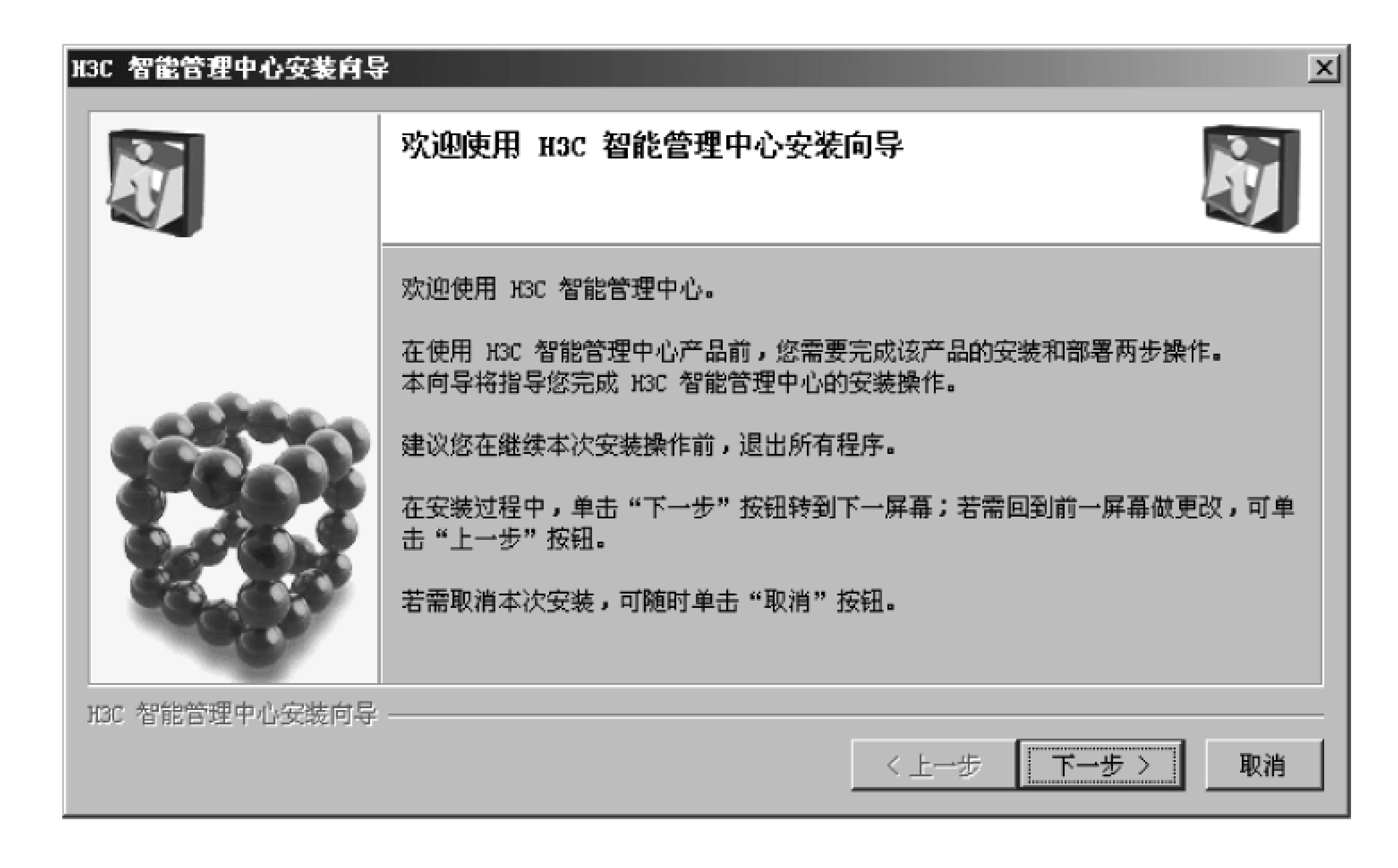


图C-1　“选择国家/地区和语言”对话框



图C-2　“检查数据库连接”对话框

在图C-2中输入数据库“sa”用户密码并单击“确定”按钮,开始检查数据库连接。在安装环境检查通过后,进入“欢迎使用H3C智能管理中心安装向导”界面,如图C-3所示。



图C-3　“欢迎使用H3C智能管理中心安装向导”界面

在图 C-3 中单击“下一步”按钮，进入“许可协议”界面，如图 C-4 所示。



图 C-4　“许可协议”界面

在图 C-4 中选择“我同意”单选按钮，然后单击“下一步”按钮，系统开始检查当前的组件安装情况，检查完成后进入“安装目标文件夹”界面，如图 C-5 所示。



图 C-5　“安装目标文件夹”界面

在图 C-5 中可以选择 iMC 的安装路径,默认路径为“C:\Program Files\iMC”。在安装 iMC 的分区下至少应该保留 5GB 的可用磁盘空间。选择安装路径后,单击“下一步”按钮进入“安装摘要信息”界面,在该对话框中将显示每一个即将安装的组件的名称、描述、版本号和所需磁盘空间等,在最后还将显示 iMC 的安装位置、安装所需的全部磁盘空间以及安装 iMC 的分区下当前可用的磁盘空间大小等信息,如图 C-6 所示。



图 C-6 “安装摘要信息”界面

在图 C-6 中单击“开始安装”按钮,进入“正在执行安装操作”界面,如图 C-7 所示。



图 C-7 “正在执行安装操作”界面

安装过程可能要花费数分钟的时间，安装完成后进入“安装完成”界面，如图 C-8 所示。

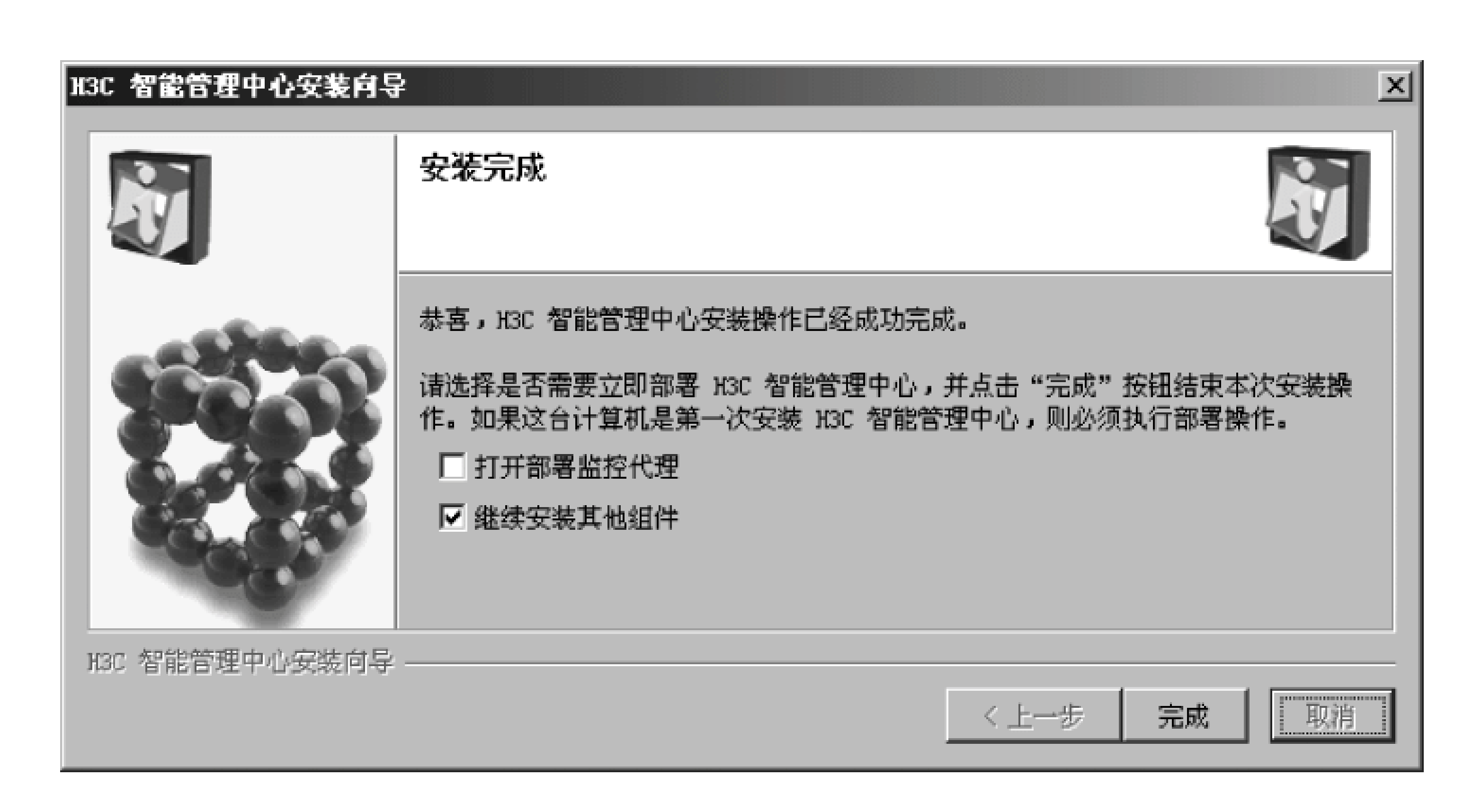


图 C-8　“安装完成”界面

至此，iMC 的智能管理平台安装完成，如果需要安装业务组件，在图 C-8 中选中“继续安装其他组件”复选框并单击“完成”按钮将继续进行业务组件的安装。

C.3　iMC 的部署过程

iMC 的安装过程实际上是一个文件复制并启动部署代理的过程，iMC 各个组件的功能必须要经过部署才能使用。为方便用户的部署操作，iMC 提供了批量部署功能。在图 C-8 的“安装完成”对话框中选中“打开部署监控代理”复选框并单击“完成”按钮，系统会自动启动智能部署监控代理，并弹出“批量部署”界面，如图 C-9 所示。



图 C-9　“批量部署”界面

在图C-9中可以选择需要部署的组件,单击“确定”按钮进入“数据库配置信息”界面,如图C-10所示。



图C-10 “数据库配置信息”界面

在图C-10中输入“sa”用户密码,并可选择数据文件的存放位置,默认存放位置为“C:\Program Files\imcdata”。单击“下一步”按钮进入“配置Web服务端口”界面,如图C-11所示。



图C-11 “配置Web服务端口”界面

默认情况下,HTTP端口为8080,HTTPS端口为8443,用户可以根据需要将其修改为其他端口。单击“开始部署”按钮,系统开始执行部署操作,如图C-12所示。

部署完成后,弹出“批量部署操作成功”界面,如图C-13所示。

在图C-13中选中“立即启动iMC服务”复选框并单击“确定”按钮,系统会立即启动iMC服务。在系统自动弹出的“智能部署监控代理”对话框中,选择“部署”标签,可以看



图 C-12 “正在执行部署操作”界面

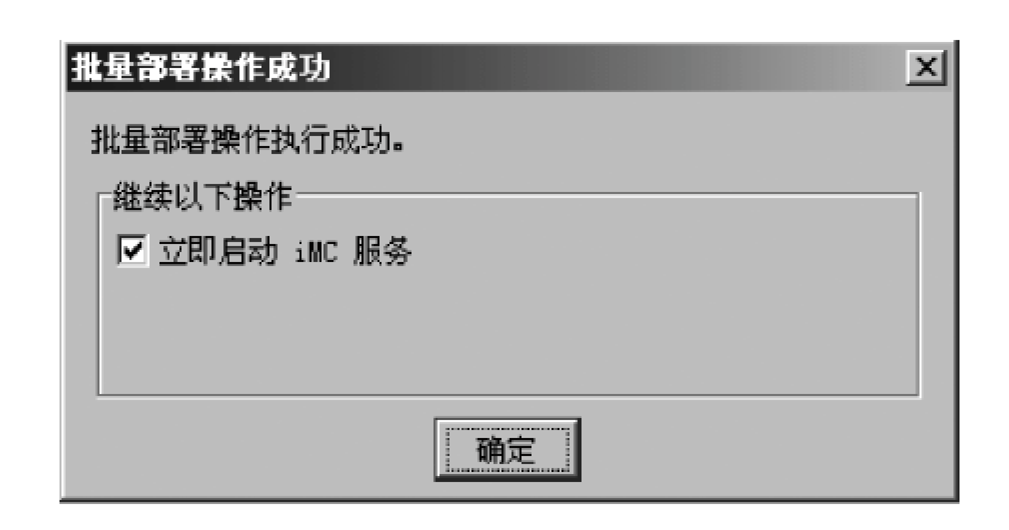


图 C-13 “批量部署操作成功”界面

到各个组件的部署信息，如图C-14所示。

智能部署监控代理

监控 | 进程 | 部署 | 运行环境

组件名	描述	版本	状态	部署位置
智能管理平台 - 资源管理	对网络中的路由器、交换机等各...	3.20-R2606	已部署	主服务器
智能管理平台 - 告警管理	对网络进行故障监控，及时分析...	3.20-R2606	已部署	主服务器
智能管理平台 - 数据分析管理	管理数据分析工程和任务。	3.20-R2606	已部署	主服务器
智能管理平台 - 数据分析服务器	在数据存储之间提供数据抽取、...	3.20-R2606	已部署	主服务器
智能管理平台 - 来宾接入管理	对来宾帐号进行全面、智能、安...	3.20-R2606	未部署	
智能管理平台 - 性能管理	对网络进行性能监控分析。	3.20-R2606	已部署	主服务器
智能管理平台 - 网络资产管理	对网络中的设备及其配件资产进...	3.20-R2606	未部署	
智能管理平台 - ACL管理	对设备进行ACL配置，实现网络数...	3.20-R2606	未部署	
智能管理平台 - 智能配置中心	对网络设备进行软件升级、设备...	3.20-R2606	已部署	主服务器
智能管理平台 - 网元管理	提供对数据通信设备如以太网交...	3.20-R2606	已部署	主服务器
智能管理平台 - 报表管理	提供各类业务报表的发布、展示...	3.20-R2606	已部署	主服务器
智能管理平台 - 安全控制中心	监控网络中的各种事件，提供安...	3.20-R2606	已部署	主服务器
智能管理平台 - Syslog管理	对设备Syslog进行收集、过滤、...	3.20-R2606	未部署	
智能管理平台 - VLAN管理	对网络中VLAN资源进行管理。	3.20-R2606	未部署	
智能管理平台 - 数据分析服务器	在数据存储之间提供数据抽取、...	3.20-R2606	未部署	

请选择组件，按下鼠标右键激活操作菜单。

图 C-14 组件部署信息

在所有的组件均部署完成后,选择"监控"标签,可以看到当前 iMC 已经启动,并且可以实时监控磁盘、CPU 和物理内存的使用情况,如图 C-15 所示。



图 C-15 iMC 监控信息

此时,在 IE 浏览器中输入地址 http://localhost:8080/imc 即可进入 iMC 的登录界面。

C.4 iMC 的注册过程

iMC 安装和部署完成后,需要进行注册方可长期使用,如果不进行注册则只能够试用 45 天。iMC 的注册方法如下。

在 iMC 的登录界面下单击"产品注册"链接,进入注册操作选择对话框,如图 C-16 所示。



图 C-16 注册操作选择对话框

在图 C-16 中输入 admin 的登录密码,并选择要执行的操作为"申请新的 License 或升级现有的 License",单击"下一步"按钮进入用户信息输入对话框,如图 C-17 所示。

请按以下要求输入您的用户信息

最终用户的信息

* 用户姓名

* 国家/地区　中国

* 省/市

* 公司或单位名称

地址

邮编

电子邮件地址

联系电话

申请人的信息

* 姓名

* 公司或单位名称

* 电子邮件地址

* 联系电话

License Keys

新的License Key　增加

License Keys列表　删除

上一步　确定　取消

图 C-17　用户信息输入对话框

在图 C-17 中输入最终用户信息、申请人信息和 License Keys 数据，其中 License Keys 可以在 H3C 提供的软件使用授权书上找到。输入完成后，单击“确定”按钮进入“用户信息收集成功”对话框，如图 C-18 所示。

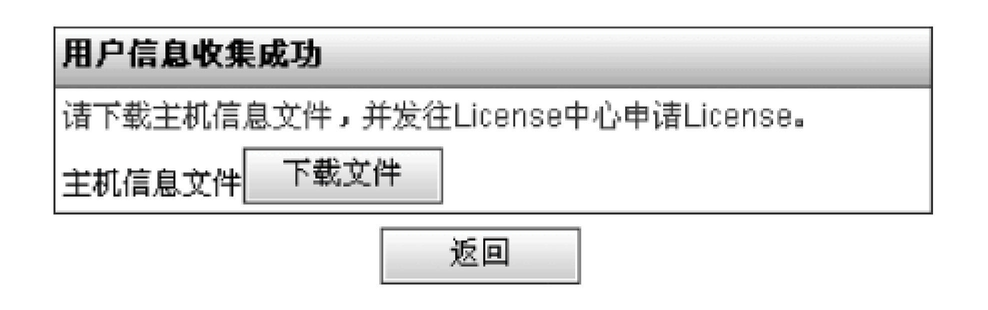


图 C-18　“用户信息收集成功”对话框

在图 C-18 中单击“下载文件”按钮，将主机信息文件下载到本地并将其发送到电子邮箱 license@h3c.com 申请获得 iMC 许可证。主机信息文件为密文，如图 C-19 所示。

在获取了 iMC 许可证后，在 iMC 的登录界面下单击“产品注册”链接，进入“选择您的操作选择”对话框，并选择要执行的操作为“使用 License 文件对产品进行注册”，如图 C-20 所示。

在图 C-20 中单击“下一步”按钮进入“注册您的产品”对话框，如图 C-21 所示。

在图 C-21 中选择 H3C 下发的许可证 License 文件后单击“确定”按钮完成 iMC 的注册操作。

在注册完成后，需要重新启动 iMC，注册信息方可生效。



图 C-19　主机信息文件内容



图 C-20　选择对 iMC 进行注册操作

注册您的产品

* License文件　浏览...

* 请您选择License类型　注册为主机License

上一步　确定　取消

图 C-21　“注册您的产品”对话框

参考文献

[1] 杭州华三通信技术有限公司.路由与交换技术 第1卷(下册)[M].北京:清华大学出版社,2011.

[2] 杭州华三通信技术有限公司. H3C 网络安全技术. 北京:杭州华三通信技术有限公司培训中心,2010.

[3] 杭州华三通信技术有限公司. H3C官方网站文档中心.杭州:杭州华三通信技术有限公司,2012.

[4] 杭州华三通信技术有限公司. H3C 智能管理中心用户手册. 杭州:杭州华三通信技术有限公司,2011.

[5] 田庚林,田华,张少芳.计算机网络安全与管理[M].北京:清华大学出版社,2010.